LACHLAN SHIRE COUNCIL

Wiradjuri Country

ATTACHMENTS

Ordinary Council Meeting

17 July 2024

Table of Contents

LACHLAN SHIRE COUNCIL
Wiradjuri Country

Investment Report

01/06/2024 to 30/06/2024

Portfolio Valuation as at 30/06/2024

Issuer	Rating	Type	Allocation	Interest Paid	Purchase Date	Maturity Date	Rate (%)	Capital Value ($)	Face Value ($)	Accrued ($)	Accrued MTD ($)
Westpac	AA-	TD	GENERAL	Quarterly	06/07/2021	09/07/2024	0.8000	1,000,000.00	1,000,000.00	1,841.10	657.53
Commonwealth Bank	AA-	TD	GENERAL	Semi-Annual	20/07/2022	23/07/2024	4.3700	1,000,000.00	1,000,000.00	19,275.89	3,591.78
Heritage and Peoples Choice Limited	BBB+	TD	GENERAL	Annual	25/07/2023	24/07/2024	5.7000	1,000,000.00	1,000,000.00	53,408.22	4,684.93
NAB	AA-	TD	GENERAL	Annual	26/07/2023	30/07/2024	5.5000	600,000.00	600,000.00	30,830.14	2,712.33
AMP Bank	BBB+	TD	GENERAL	Annual	08/08/2023	13/08/2024	5.4500	1,000,000.00	1,000,000.00	48,975.34	4,479.45
AMP Bank	BBB+	TD	GENERAL	Annual	15/08/2023	20/08/2024	5.3000	1,000,000.00	1,000,000.00	46,610.96	4,356.16
Westpac	AA-	TD	GENERAL	Quarterly	23/08/2022	23/08/2024	4.3800	500,000.00	500,000.00	2,340.00	1,800.00
Australian Military Bank	BBB+	TD	GENERAL	Quarterly	29/08/2022	29/08/2024	4.4500	1,000,000.00	1,000,000.00	4,023.29	3,657.53
NAB	AA-	TD	GENERAL	At Maturity	31/08/2023	03/09/2024	5.2200	1,000,000.00	1,000,000.00	43,619.18	4,290.41
Westpac	AA-	TD	GENERAL	Quarterly	30/08/2022	03/09/2024	4.4400	1,000,000.00	1,000,000.00	3,892.60	3,649.32
BOQ	A-	TD	GENERAL	At Maturity	30/08/2022	03/09/2024	4.4000	1,000,000.00	1,000,000.00	80,887.67	3,616.44
NAB	AA-	TD	GENERAL	Quarterly	05/09/2023	10/09/2024	5.2000	1,000,000.00	1,000,000.00	3,704.11	3,704.11
P&N Bank	BBB+	TD	GENERAL	Quarterly	08/09/2022	10/09/2024	4.4000	1,500,000.00	1,500,000.00	3,616.44	3,616.44
P&N Bank	BBB+	TD	GENERAL	Annual	13/09/2022	13/09/2024	4.4500	500,000.00	500,000.00	17,800.00	1,828.77
NAB	AA-	TD	GENERAL	Annual	13/09/2023	17/09/2024	5.2400	1,500,000.00	1,500,000.00	62,880.00	6,460.27
BOQ	A-	TD	GENERAL	Annual	27/03/2024	24/09/2024	5.0900	1,000,000.00	1,000,000.00	13,387.40	4,183.56
AMP Bank	BBB+	TD	GENERAL	Annual	20/10/2022	21/10/2024	4.9000	1,000,000.00	1,000,000.00	34,232.88	4,027.40
ING Bank (Australia)	A	TD	GENERAL	Annual	07/11/2023	05/11/2024	5.4800	1,000,000.00	1,000,000.00	35,582.47	4,504.11

Issuer	Rating	Type	Allocation	Interest Paid	Purchase Date	Maturity Date	Rate (%)	Capital Value ($)	Face Value ($)	Accrued ($)	Accrued MTD ($)
Ltd											
AMP Bank	BBB+	TD	GENERAL	Annual	22/11/2022	19/11/2024	4.7000	750,000.00	750,000.00	21,439.73	2,897.26
AMP Bank	BBB+	TD	GENERAL	Annual	29/11/2022	03/12/2024	4.6500	1,000,000.00	1,000,000.00	27,390.41	3,821.92
Westpac	AA-	TD	GENERAL	Quarterly	05/12/2023	05/12/2024	5.3000	750,000.00	750,000.00	2,831.51	2,831.51
BOQ	A-	TD	GENERAL	Annual	11/12/2023	10/12/2024	5.3200	1,500,000.00	1,500,000.00	44,381.92	6,558.90
Bank of Sydney	Unrated	TD	GENERAL	Annual	12/12/2023	12/12/2024	5.3500	500,000.00	500,000.00	14,804.11	2,198.63
Westpac	AA-	TD	GENERAL	Quarterly	13/02/2024	18/02/2025	5.1200	500,000.00	500,000.00	3,436.71	2,104.11
P&N Bank	BBB+	TD	GENERAL	Annual	21/02/2023	25/02/2025	5.0000	1,000,000.00	1,000,000.00	17,945.21	4,109.59
Bank of Sydney	Unrated	TD	GENERAL	At Maturity	27/02/2024	26/02/2025	5.1700	500,000.00	500,000.00	8,852.74	2,124.66
ING Bank (Australia) Ltd	A	TD	GENERAL	Annual	02/03/2023	04/03/2025	5.1000	500,000.00	500,000.00	8,313.70	2,095.89
Police Credit Union SA	Unrated	TD	GENERAL	At Maturity	14/03/2023	18/03/2025	4.9400	1,000,000.00	1,000,000.00	64,287.67	4,060.27
Westpac	AA-	TD	GENERAL	Quarterly	26/03/2024	26/03/2025	4.9700	1,000,000.00	1,000,000.00	680.82	680.82
Summerland Bank	Unrated	TD	GENERAL	Annual	29/03/2023	01/04/2025	4.8700	1,000,000.00	1,000,000.00	12,675.34	4,002.74
Auswide Bank	BBB	TD	GENERAL	Annual	04/04/2023	08/04/2025	4.9000	900,000.00	900,000.00	10,632.33	3,624.66
AMP Bank	BBB+	TD	GENERAL	Annual	09/05/2023	06/05/2025	5.0000	1,000,000.00	1,000,000.00	7,260.27	4,109.59
ING Bank (Australia) Ltd	A	TD	GENERAL	At Maturity	28/05/2024	27/05/2025	5.2700	1,000,000.00	1,000,000.00	4,909.04	4,331.51
ING Bank (Australia) Ltd	A	TD	GENERAL	Annual	28/06/2023	26/06/2025	5.5500	1,000,000.00	1,000,000.00	456.16	456.16
NAB	AA-	TD	GENERAL	Annual	26/06/2024	26/06/2025	5.3000	1,000,000.00	1,000,000.00	726.03	726.03
NAB	AA-	TD	GENERAL	Annual	27/06/2024	02/07/2025	5.5000	1,000,000.00	1,000,000.00	602.74	602.74

Issuer	Rating	Type	Allocation	Interest Paid	Purchase Date	Maturity Date	Rate (%)	Capital Value ($)	Face Value ($)	Accrued ($)	Accrued MTD ($)
P&N Bank	BBB+	TD	GENERAL	Annual	11/07/2023	09/07/2025	5.8000	1,000,000.00	1,000,000.00	56,569.86	4,767.12
BOQ	A-	TD	GENERAL	Annual	10/08/2021	12/08/2025	1.0000	1,000,000.00	1,000,000.00	8,931.51	821.92
ING Bank (Australia) Ltd	A	TD	GENERAL	Annual	05/09/2023	09/09/2025	5.0500	500,000.00	500,000.00	20,753.42	2,075.34
Westpac	AA-	TD	GENERAL	Quarterly	12/09/2023	16/09/2025	5.0200	1,500,000.00	1,500,000.00	3,919.73	3,919.73
ING Bank (Australia) Ltd	A	TD	GENERAL	At Maturity	28/09/2023	30/09/2025	5.2500	1,000,000.00	1,000,000.00	39,842.47	4,315.07
ING Bank (Australia) Ltd	A	TD	GENERAL	At Maturity	04/10/2023	07/10/2025	5.3000	1,000,000.00	1,000,000.00	39,350.68	4,356.16
P&N Bank	BBB+	TD	GENERAL	Annual	29/11/2023	28/11/2025	5.4500	1,000,000.00	1,000,000.00	32,102.74	4,479.45
ING Bank (Australia) Ltd	A	TD	GENERAL	Annual	30/11/2023	02/12/2025	5.4200	1,000,000.00	1,000,000.00	31,777.53	4,454.79
Warwick Credit Union	Unrated	TD	GENERAL	Annual	20/12/2023	18/12/2025	5.2000	2,000,000.00	2,000,000.00	55,276.71	8,547.95
Suncorp Bank	A+	TD	GENERAL	Annual	23/01/2024	27/01/2026	5.0500	2,000,000.00	2,000,000.00	44,273.97	8,301.37
Suncorp Bank	A+	TD	GENERAL	Annual	06/02/2024	10/02/2026	4.9300	2,000,000.00	2,000,000.00	39,440.00	8,104.11
ING Bank (Australia) Ltd	A	TD	GENERAL	Annual	09/04/2024	14/04/2026	4.9300	1,000,000.00	1,000,000.00	11,210.68	4,052.05
ING Bank (Australia) Ltd	A	TD	GENERAL	At Maturity	06/06/2024	10/06/2026	5.2500	1,000,000.00	1,000,000.00	3,595.89	3,595.89
Westpac	AA-	TD	GENERAL	Annual	27/06/2024	29/06/2026	5.2500	2,000,000.00	2,000,000.00	1,150.68	1,150.68
P&N Bank	BBB+	TD	GENERAL	Annual	18/04/2023	20/04/2027	5.0000	1,000,000.00	1,000,000.00	10,136.99	4,109.59
P&N Bank	BBB+	TD	GENERAL	Annual	14/02/2023	15/02/2028	5.2000	500,000.00	500,000.00	9,830.14	2,136.99
NAB	AA-	CASH	GENERAL	Monthly	30/06/2024	30/06/2024	3.7500	3,521,656.71	3,521,656.71	10,820.72	10,820.72
Macquarie Bank	A+	CASH	GENERAL	Monthly	30/06/2024	30/06/2024	4.1500	3,887,910.87	3,887,910.87	13,218.42	13,218.42

Issuer	Rating	Type	Allocation	Interest Paid	Purchase Date	Maturity Date	Rate (%)	Capital Value ($)	Face Value ($)	Accrued ($)	Accrued MTD ($)
NAB	AA-	CASH	GENERAL	Monthly	30/06/2024	30/06/2024	2.8500	1,301,809.14	1,301,809.14	3,835.18	3,835.18
TOTALS								**61,711,376.72**	**61,711,376.72**	**1,194,571.44**	**214,220.07**

Portfolio by Asset as at 30/06/2024

Asset Type: CASH

Issuer	Rating	Type	Allocation	Interest Paid	Purchase Date	Maturity Date	Rate (%)	Capital Value ($)	Face Value ($)	Accrued ($)	Accrued MTD ($)
NAB	AA-	CASH	GENERAL	Monthly	30/06/2024	30/06/2024	3.7500	3,521,656.71	3,521,656.71	10,820.72	10,820.72
Macquarie Bank	A+	CASH	GENERAL	Monthly	30/06/2024	30/06/2024	4.1500	3,887,910.87	3,887,910.87	13,218.42	13,218.42
NAB	AA-	CASH	GENERAL	Monthly	30/06/2024	30/06/2024	2.8500	1,301,809.14	1,301,809.14	3,835.18	3,835.18
CASH SUBTOTALS								**8,711,376.72**	**8,711,376.72**	**27,874.32**	**27,874.32**

Asset Type: TD

Issuer	Rating	Type	Allocation	Interest Paid	Purchase Date	Maturity Date	Rate (%)	Capital Value ($)	Face Value ($)	Accrued ($)	Accrued MTD ($)
Westpac	AA-	TD	GENERAL	Quarterly	06/07/2021	09/07/2024	0.8000	1,000,000.00	1,000,000.00	1,841.10	657.53
Commonwealth Bank	AA-	TD	GENERAL	Semi-Annual	20/07/2022	23/07/2024	4.3700	1,000,000.00	1,000,000.00	19,275.89	3,591.78
Heritage and Peoples Choice Limited	BBB+	TD	GENERAL	Annual	25/07/2023	24/07/2024	5.7000	1,000,000.00	1,000,000.00	53,408.22	4,684.93
NAB	AA-	TD	GENERAL	Annual	26/07/2023	30/07/2024	5.5000	600,000.00	600,000.00	30,830.14	2,712.33
AMP Bank	BBB+	TD	GENERAL	Annual	08/08/2023	13/08/2024	5.4500	1,000,000.00	1,000,000.00	48,975.34	4,479.45
AMP Bank	BBB+	TD	GENERAL	Annual	15/08/2023	20/08/2024	5.3000	1,000,000.00	1,000,000.00	46,610.96	4,356.16
Westpac	AA-	TD	GENERAL	Quarterly	23/08/2022	23/08/2024	4.3800	500,000.00	500,000.00	2,340.00	1,800.00
Australian Military Bank	BBB+	TD	GENERAL	Quarterly	29/08/2022	29/08/2024	4.4500	1,000,000.00	1,000,000.00	4,023.29	3,657.53
NAB	AA-	TD	GENERAL	At Maturity	31/08/2023	03/09/2024	5.2200	1,000,000.00	1,000,000.00	43,619.18	4,290.41

Issuer	Rating	Type	Allocation	Interest Paid	Purchase Date	Maturity Date	Rate (%)	Capital Value ($)	Face Value ($)	Accrued ($)	Accrued MTD ($)
Westpac	AA-	TD	GENERAL	Quarterly	30/08/2022	03/09/2024	4.4400	1,000,000.00	1,000,000.00	3,892.60	3,649.32
BOQ	A-	TD	GENERAL	At Maturity	30/08/2022	03/09/2024	4.4000	1,000,000.00	1,000,000.00	80,887.67	3,616.44
NAB	AA-	TD	GENERAL	Quarterly	05/09/2023	10/09/2024	5.2000	1,000,000.00	1,000,000.00	3,704.11	3,704.11
P&N Bank	BBB+	TD	GENERAL	Quarterly	08/09/2022	10/09/2024	4.4000	1,500,000.00	1,500,000.00	3,616.44	3,616.44
P&N Bank	BBB+	TD	GENERAL	Annual	13/09/2022	13/09/2024	4.4500	500,000.00	500,000.00	17,800.00	1,828.77
NAB	AA-	TD	GENERAL	Annual	13/09/2023	17/09/2024	5.2400	1,500,000.00	1,500,000.00	62,880.00	6,460.27
BOQ	A-	TD	GENERAL	Annual	27/03/2024	24/09/2024	5.0900	1,000,000.00	1,000,000.00	13,387.40	4,183.56
AMP Bank	BBB+	TD	GENERAL	Annual	20/10/2022	21/10/2024	4.9000	1,000,000.00	1,000,000.00	34,232.88	4,027.40
ING Bank (Australia) Ltd	A	TD	GENERAL	Annual	07/11/2023	05/11/2024	5.4800	1,000,000.00	1,000,000.00	35,582.47	4,504.11
AMP Bank	BBB+	TD	GENERAL	Annual	22/11/2022	19/11/2024	4.7000	750,000.00	750,000.00	21,439.73	2,897.26
AMP Bank	BBB+	TD	GENERAL	Annual	29/11/2022	03/12/2024	4.6500	1,000,000.00	1,000,000.00	27,390.41	3,821.92
Westpac	AA-	TD	GENERAL	Quarterly	05/12/2023	05/12/2024	5.3000	750,000.00	750,000.00	2,831.51	2,831.51
BOQ	A-	TD	GENERAL	Annual	11/12/2023	10/12/2024	5.3200	1,500,000.00	1,500,000.00	44,381.92	6,558.90
Bank of Sydney	Unrated	TD	GENERAL	Annual	12/12/2023	12/12/2024	5.3500	500,000.00	500,000.00	14,804.11	2,198.63
Westpac	AA-	TD	GENERAL	Quarterly	13/02/2024	18/02/2025	5.1200	500,000.00	500,000.00	3,436.71	2,104.11
P&N Bank	BBB+	TD	GENERAL	Annual	21/02/2023	25/02/2025	5.0000	1,000,000.00	1,000,000.00	17,945.21	4,109.59
Bank of Sydney	Unrated	TD	GENERAL	At Maturity	27/02/2024	26/02/2025	5.1700	500,000.00	500,000.00	8,852.74	2,124.66
ING Bank (Australia) Ltd	A	TD	GENERAL	Annual	02/03/2023	04/03/2025	5.1000	500,000.00	500,000.00	8,313.70	2,095.89
Police Credit Union SA	Unrated	TD	GENERAL	At Maturity	14/03/2023	18/03/2025	4.9400	1,000,000.00	1,000,000.00	64,287.67	4,060.27

Issuer	Rating	Type	Allocation	Interest Paid	Purchase Date	Maturity Date	Rate (%)	Capital Value ($)	Face Value ($)	Accrued ($)	Accrued MTD ($)
Westpac	AA-	TD	GENERAL	Quarterly	26/03/2024	26/03/2025	4.9700	1,000,000.00	1,000,000.00	680.82	680.82
Summerland Bank	Unrated	TD	GENERAL	Annual	29/03/2023	01/04/2025	4.8700	1,000,000.00	1,000,000.00	12,675.34	4,002.74
Auswide Bank	BBB	TD	GENERAL	Annual	04/04/2023	08/04/2025	4.9000	900,000.00	900,000.00	10,632.33	3,624.66
AMP Bank	BBB+	TD	GENERAL	Annual	09/05/2023	06/05/2025	5.0000	1,000,000.00	1,000,000.00	7,260.27	4,109.59
ING Bank (Australia) Ltd	A	TD	GENERAL	At Maturity	28/05/2024	27/05/2025	5.2700	1,000,000.00	1,000,000.00	4,909.04	4,331.51
ING Bank (Australia) Ltd	A	TD	GENERAL	Annual	28/06/2023	26/06/2025	5.5500	1,000,000.00	1,000,000.00	456.16	456.16
NAB	AA-	TD	GENERAL	Annual	26/06/2024	26/06/2025	5.3000	1,000,000.00	1,000,000.00	726.03	726.03
NAB	AA-	TD	GENERAL	Annual	27/06/2024	02/07/2025	5.5000	1,000,000.00	1,000,000.00	602.74	602.74
P&N Bank	BBB+	TD	GENERAL	Annual	11/07/2023	09/07/2025	5.8000	1,000,000.00	1,000,000.00	56,569.86	4,767.12
BOQ	A-	TD	GENERAL	Annual	10/08/2021	12/08/2025	1.0000	1,000,000.00	1,000,000.00	8,931.51	821.92
ING Bank (Australia) Ltd	A	TD	GENERAL	Annual	05/09/2023	09/09/2025	5.0500	500,000.00	500,000.00	20,753.42	2,075.34
Westpac	AA-	TD	GENERAL	Quarterly	12/09/2023	16/09/2025	5.0200	1,500,000.00	1,500,000.00	3,919.73	3,919.73
ING Bank (Australia) Ltd	A	TD	GENERAL	At Maturity	28/09/2023	30/09/2025	5.2500	1,000,000.00	1,000,000.00	39,842.47	4,315.07
ING Bank (Australia) Ltd	A	TD	GENERAL	At Maturity	04/10/2023	07/10/2025	5.3000	1,000,000.00	1,000,000.00	39,350.68	4,356.16
P&N Bank	BBB+	TD	GENERAL	Annual	29/11/2023	28/11/2025	5.4500	1,000,000.00	1,000,000.00	32,102.74	4,479.45
ING Bank (Australia) Ltd	A	TD	GENERAL	Annual	30/11/2023	02/12/2025	5.4200	1,000,000.00	1,000,000.00	31,777.53	4,454.79
Warwick Credit Union	Unrated	TD	GENERAL	Annual	20/12/2023	18/12/2025	5.2000	2,000,000.00	2,000,000.00	55,276.71	8,547.95
Suncorp Bank	A+	TD	GENERAL	Annual	23/01/2024	27/01/2026	5.0500	2,000,000.00	2,000,000.00	44,273.97	8,301.37

Issuer	Rating	Type	Allocation	Interest Paid	Purchase Date	Maturity Date	Rate (%)	Capital Value ($)	Face Value ($)	Accrued ($)	Accrued MTD ($)
Suncorp Bank	A+	TD	GENERAL	Annual	06/02/2024	10/02/2026	4.9300	2,000,000.00	2,000,000.00	39,440.00	8,104.11
ING Bank (Australia) Ltd	A	TD	GENERAL	Annual	09/04/2024	14/04/2026	4.9300	1,000,000.00	1,000,000.00	11,210.68	4,052.05
ING Bank (Australia) Ltd	A	TD	GENERAL	At Maturity	06/06/2024	10/06/2026	5.2500	1,000,000.00	1,000,000.00	3,595.89	3,595.89
Westpac	AA-	TD	GENERAL	Annual	27/06/2024	29/06/2026	5.2500	2,000,000.00	2,000,000.00	1,150.68	1,150.68
P&N Bank	BBB+	TD	GENERAL	Annual	18/04/2023	20/04/2027	5.0000	1,000,000.00	1,000,000.00	10,136.99	4,109.59
P&N Bank	BBB+	TD	GENERAL	Annual	14/02/2023	15/02/2028	5.2000	500,000.00	500,000.00	9,830.14	2,136.99
TD SUBTOTALS								**53,000,000.00**	**53,000,000.00**	**1,166,697.12**	**186,345.75**

Portfolio by Asset Totals as at 30/06/2024

Type	Capital Value ($)	Face Value ($)	Accrued ($)	Accrued MTD ($)
CASH	8,711,376.72	8,711,376.72	27,874.32	27,874.32
TD	53,000,000.00	53,000,000.00	1,166,697.12	186,345.75
TOTALS	**61,711,376.72**	**61,711,376.72**	**1,194,571.44**	**214,220.07**

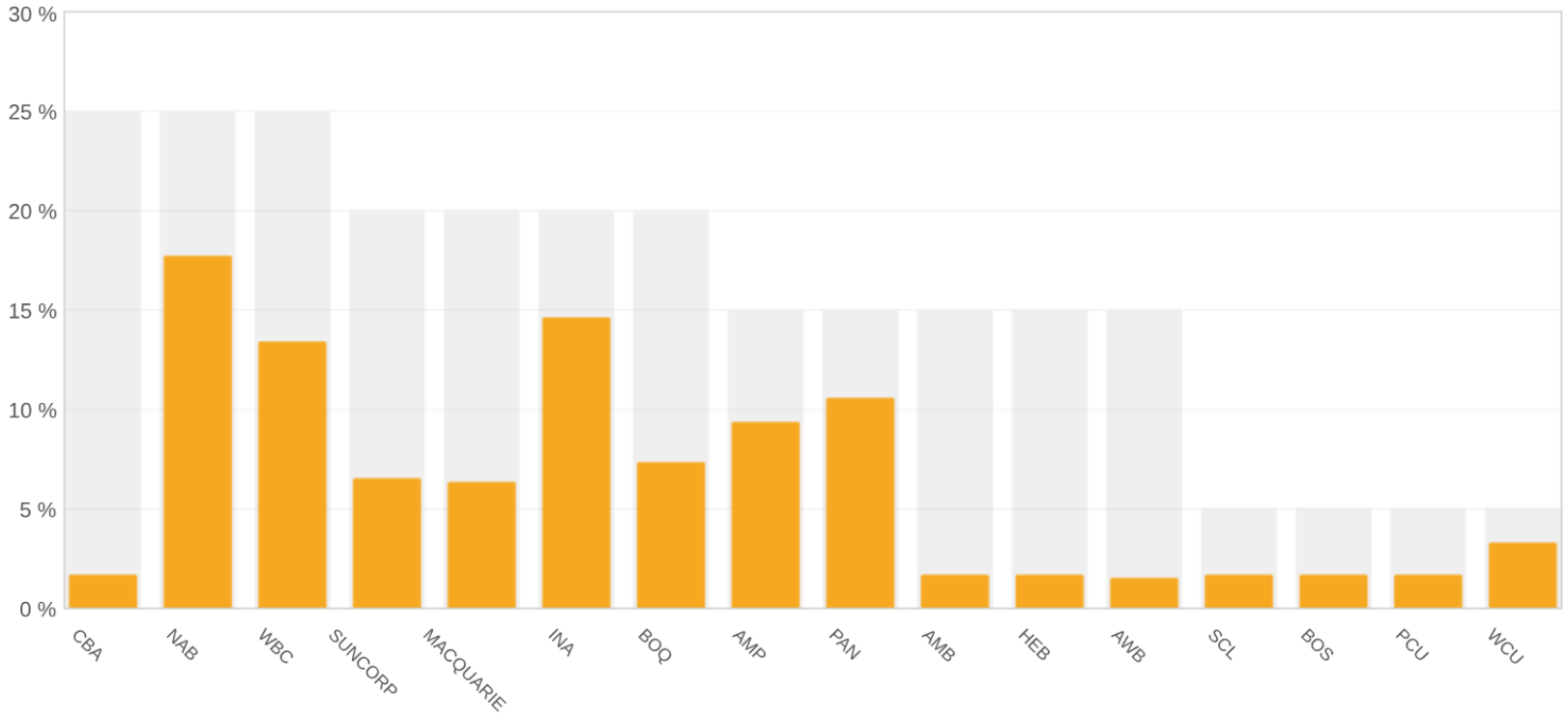
Counterparty Compliance as at 30/06/2024

Long Term Investments

Compliant	Bank Group	Term	Rating	Invested ($)	Invested (%)	Limit (%)	Limit ($)	Available ($)
✔	Commonwealth Bank	Long	AA-	1,000,000.00	1.62	25.00	-	14,427,844.18
✔	NAB	Long	AA-	10,923,465.85	17.70	25.00	-	4,504,378.33
✔	Westpac	Long	AA-	8,250,000.00	13.37	25.00	-	7,177,844.18
✔	Suncorp	Long	A+	4,000,000.00	6.48	20.00	-	8,342,275.34
✔	Macquarie Bank	Long	A+	3,887,910.87	6.30	20.00	-	8,454,364.47
✔	ING Bank (Australia) Ltd	Long	A	9,000,000.00	14.58	20.00	-	3,342,275.34
✔	BOQ	Long	A-	4,500,000.00	7.29	20.00	-	7,842,275.34
✔	AMP Bank	Long	BBB+	5,750,000.00	9.32	15.00	-	3,506,706.51
✔	P&N Bank	Long	BBB+	6,500,000.00	10.53	15.00	-	2,756,706.51
✔	Australian Military Bank	Long	BBB+	1,000,000.00	1.62	15.00	-	8,256,706.51
✔	Heritage Bank	Long	BBB+	1,000,000.00	1.62	15.00	-	8,256,706.51
✔	Auswide Bank	Long	BBB	900,000.00	1.46	15.00	-	8,356,706.51
✔	Summerland Credit Union	Long	Unrated	1,000,000.00	1.62	5.00	-	2,085,568.84
✔	Bank of Sydney	Long	Unrated	1,000,000.00	1.62	5.00	-	2,085,568.84

Compliant	Bank Group	Term	Rating	Invested ($)	Invested (%)	Limit (%)	Limit ($)	Available ($)
✔	Police Credit Union SA	Long	Unrated	1,000,000.00	1.62	5.00	-	2,085,568.84
✔	Warwick Credit Union	Long	Unrated	2,000,000.00	3.24	5.00	-	1,085,568.84
TOTALS				**61,711,376.72**	**100.00**			

Counterparty Compliance - Long Term Investments

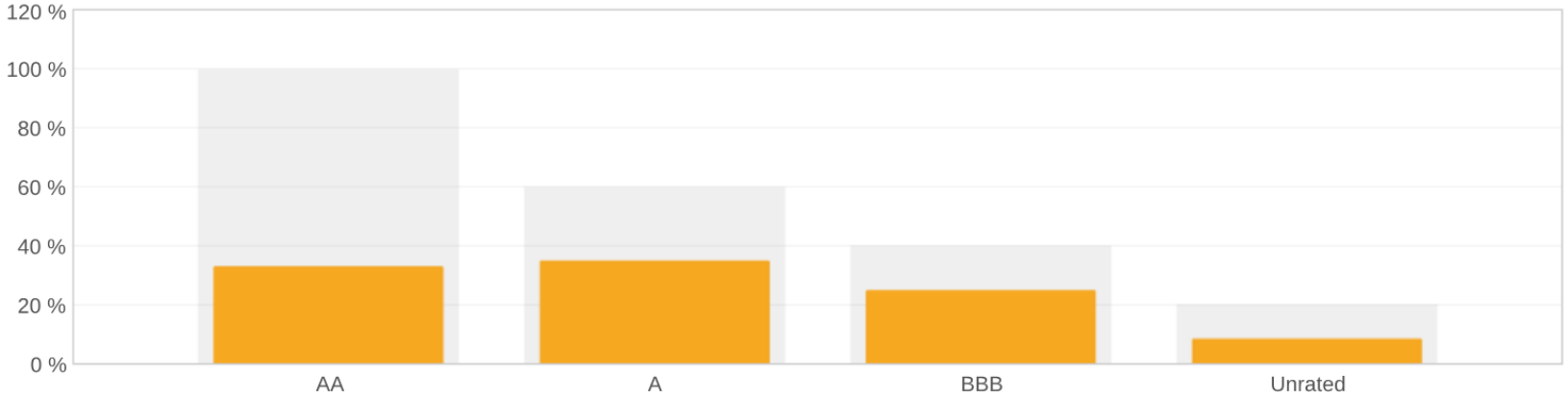


Credit Quality Compliance as at 30/06/2024

Long Term Investments

Compliant	Rating	Invested ($)	Invested (%)	Limit (%)	Available ($)
✔	AA	20,173,465.85	32.69	100.00	41,537,910.87
✔	A	21,387,910.87	34.66	60.00	15,638,915.16
✔	BBB	15,150,000.00	24.55	40.00	9,534,550.69
✔	Unrated	5,000,000.00	8.10	20.00	7,342,275.34
TOTALS		**61,711,376.72**	**100.00**		

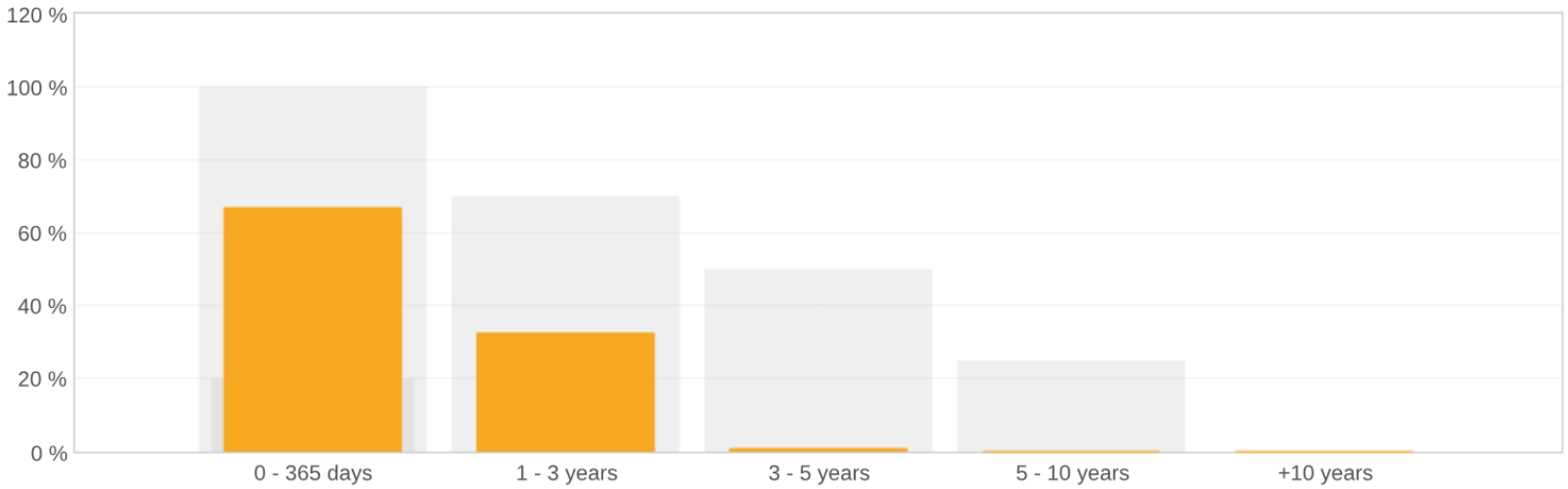
Credit Quality Compliance - Long Term Investments



Maturity Compliance as at 30/06/2024

Compliant	Term	Invested ($)	Invested (%)	Min Limit (%)	Max Limit (%)	Available ($)
✔	0 - 365 days	41,211,376.72	66.78	20.00	100.00	20,500,000.00
✔	1 - 3 years	20,000,000.00	32.41	0.00	70.00	23,197,963.70
✔	3 - 5 years	500,000.00	0.81	0.00	50.00	30,355,688.36
✔	5 - 10 years	-	0.00	0.00	25.00	15,427,844.18
✔	+10 years	-	0.00	0.00	0.00	-
TOTALS		**61,711,376.72**	**100.00**			

Maturity Compliance

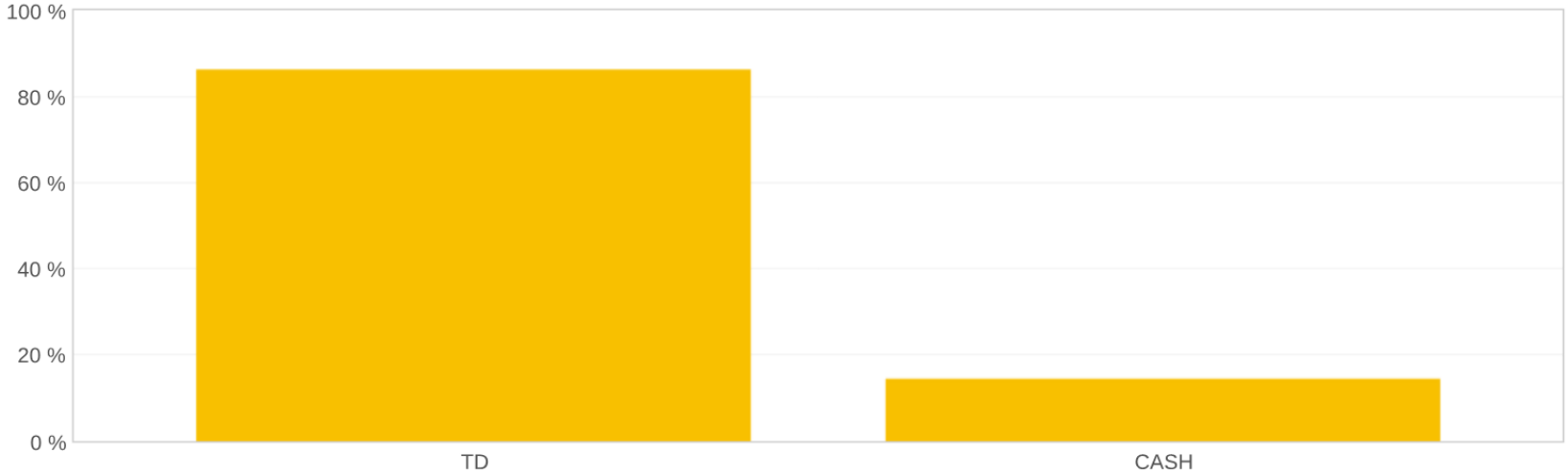


IMPERIUM MARKETS

Asset Class as at 30/06/2024

Code	Number of Trades	Invested ($)	Invested (%)
TD	52	53,000,000.00	85.88
CASH	3	8,711,376.72	14.12
TOTALS	**55**	**61,711,376.72**	**100.0**

Asset Class Distribution



ACTIVE RESOLUTIONS AS AT 17 JULY 2024

LACHLAN SHIRE COUNCIL REPORT TO COUNCIL MEETING TO BE HELD 17 JULY 2024				
AUTHOR:	**GENERAL MANAGER**			
	Dept.	**Resolution**	**Action Taken to Date**	**Expected Completion**
June 2024	GM	**2024/138 17.4 SALE OF LAND FOR UNPAID RATES - LOT 5 DP 752102** **RESOLVED THAT:** 1. The General Manager's Report No. R24/158 be received and noted. 2. Council endorse the sale of Lot 5 DP 752102 as outlined in the report. 3. The General Manager be authorised to sign the contract documents and complete the sale. **Medcalf/Mortimer**	Sale contract prepared and sale progressing.	August 2024
June 2024	GM	**2024/137 17.3 CONDOBOLIN CHILD CARE FACILITIES** **RESOLVED THAT:** 1. The General Managers Report No R24/152 be received and noted. 2. The General Manager investigate the various opportunities for the expansion of child care services in Condobolin. 3. A further report be presented to Council on the result of the investigation with a recommended strategy for Council's consideration. **Brady/Mortimer**	Meeting held with Condobolin Child Care representatives to discuss Council's resolution. Quotations requested for valuation of Child Care facility	November 2024
March 2024	GM	**2024/55 17.6 LAND ACQUISITION - JONES LANE CONDOBOLIN** **RESOLVED THAT:** 1. The General Manager's report No. R24/66 be received and noted. 2. Council resolve to pursue the compulsory acquisition of the subject property located in Jones Lane Condobolin in accordance with the	Instruction given to Council's legal representative to commence compulsory acquisition. Action deferred for 1 month following	December 2024

ACTIVE RESOLUTIONS AS AT 17 JULY 2024

		Land Acquisition (Just Terms Compensation) Act 1991 (Just Terms Act). 3. The Mayor and General Manager be delegated authority to negotiate, complete and sign any necessary documentation and affix the Council seal if required to facilitate the acquisition. 4. The General Manager be instructed and authorised to engage a legal representative to assist Council with all aspects of the acquisition. Bartholomew/Mortimer	communication from landowner's representative that they are obtaining a valuation. No further communication from landowner so legal representative instructed to issue compulsory acquisition notice. Landowners representative has advised they now have a valuation and wish to exchange valuation reports and commence negotiations.	
March 2024	GM	**2024/54 17.5 LACHLAN SHIRE COUNCIL WORKS DEPOT CONSTRUCTION ARRANGEMENTS** **RESOLVED THAT:** 1. The General Manager's Report No. R24/65 be received and noted. 2. Option 5. (Invite tenders for Project Management and Site Supervision services only. Invite separate tenders from suitable qualified tradespeople and sub-contractors for a Panel Contract) be endorsed as the preferred arrangement to complete the Depot Construction Project. Harris/Medcalf	Tender documents are being prepared. RFT should be distributed by June 2024. Survey and Geotechnical investigation undertaken to determine appropriate foundation remediation treatment. Tenders closed and are under assessment. Reports to August Council meeting	August 2024

ACTIVE RESOLUTIONS AS AT 17 JULY 2024

June 2024	DEP	**2024/124 9.3.1 PLAN OF MANAGEMENT - CROWN RESERVE 86016 (CONDOBOLIN CARAVAN PARK)** **RESOLVED THAT:** 1. The Director Environment and Planning Report No. R24/139 be received and noted. 2. The draft Plan of Management be placed on public exhibition in accordance with Section 38 Local Government Act 1993 from Friday 21 June to 5pm Friday 2 August 2024, being a period of forty three (43) days. 3. That a further report be presented to Council at the end of the public exhibition period. **Harris/Turner**	The Draft Plan of Management is currently on public exhibition.	October 2024
Maya 2024	DEP	**2024/110 17.1 19 MCDONNELL STREET, CONDOBOLIN** **RESOLVED THAT:** 1. The Director of Environment and Planning Report No. R24/114 be received and noted. 2. The General Manager be authorised to make an offer and negotiate the purchase of the property to the value detailed in option 1 of the report. 3. Funds for the purchase of the property and associated costs, as detailed in option 1 of the report, be allocated from Council's Condobolin Purchase Dwelling Capital Improvement Reserve. 4. If acquired the property be classified as operational land in Council's Land and Building Asset Register as it will be used for operational purposes.	The purchase of 19 McDonnell Street is progressing well. Contracts have been exchanged. Settlement booked for the week commencing 15 July 2024	August 2024

ACTIVE RESOLUTIONS AS AT 17 JULY 2024

		5. The Mayor and General Manager be authorised to sign the contract documents and affix the Council seal if required. Harris/Brady		
May 2024	DEP	**2024/104 9.3.1 TOTTENHAM PLANNING PROPOSAL** **RESOLVED THAT:** 1. The Director of Environment and Planning Report No. R24/74 be received and noted. 2. Council endorse the preparation and lodgement of a Planning Proposal for rezoning in Tottenham, amending Lachlan Local Environmental Plan 2013, in accordance with the Council's Industrial and Rural Lands Strategy. 3. Council approve the Planning Proposal for public authority consultation and public exhibition in accordance with any conditions imposed under the Gateway Determination. 4. Council seek authority from the Department of Planning, Housing and Industry to exercise the delegation of all functions of the relevant local plan making authority under Section 3.36 of the Environmental Planning and Assessment Act 1979 to make the local environmental plan to put into effect the Planning Proposal. 5. Authority be delegated to the General Manager to make any minor variations to the Planning Proposal, following receipt of the Gateway Determination. 6. A further report be submitted to Council following the public exhibition of the Planning Proposal detailing any submissions received during the public exhibition period. Harris/Mortimer	The Tottenham Planning Proposal has been forwarded to the Department of Planning, Housing and Infrastructure (DPHI). Preliminary feedback from DPHI has been received and is currently being discussed between Council and DPHI officers. DEP attended meeting with DPHI officers in June 2024.	Ongoing.

ACTIVE RESOLUTIONS AS AT 17 JULY 2024

March 2024	DEP	**2024/53 17.4 RIVERVIEW CARAVAN PARK MANAGEMENT - CONTRACT REMUNERATION REVIEW** **RESOLVED THAT:** 1. The Director of Environmental and Planning Report No. R24/62 be received and noted. 2. Council endorse option 1 of the report. Harris/Turner	Contracts have been signed as per the council resolution.	Completed
March 2024	DEP	**2024/50 17.1 LAKE CARGELLIGO MUSEUM – UPGRADE** **RESOLVED THAT:** 1. The Director of Environmental and Planning Report No. R24/71 be received and noted. 2. Council endorse option 2 of the report. Harris/Turner	Purchase orders have been issued for approved works. Committee have been notified of outcome of report.	September 2024
March 2024	DEP	**2024/42 9.3.2 EVOLUTION MINING OPEN CUT MINING EXTENSION APPLICATION - ROAD MAINTENCE CONTRIBUTION** **RESOLVED THAT:** 1. The Director Environment and Planning Report No. R24/54 be received and noted. 2. The offer from Evolution Mining to increase the road maintenance contribution under the Memorandum of Understanding (MoU) by 50% be accepted. 3. The Mayor and General Manager be authorised to sign the MoU variation. Harris/Medcalf	Evolution Mining has been advised of Council's resolution. Awaiting amended MoU for signing.	August 2024

ACTIVE RESOLUTIONS AS AT 17 JULY 2024

February 2024	DEP	**2024/23 17.3 53-59 BATHURST STREET, CONDOBOLIN - FORMER TARGET BUILDING** **RESOLVED THAT:** 1. The Acting Director of Environmental and Planning Report No. R24/7 be received and noted. 2. Council endorse option 3 of the report, and 3. A further report be presented to Council in regard the outcome of option 3. Bartholomew/Mortimer	See the General Manager's report to the August 2024 Council Meeting	Completed
November 2023	DEP	**2023/287 17.16 1 MCINNES STREET LAKE CARGELLIGO - MASTER PLAN UPDATE** **RESOLVED THAT:** 1. The Acting Director of Environment, Tourism and Economic Development Report No. R23/341 be received and noted. 2. Council endorse the undertaking of urban design concepts, water and sewer main investigation, stormwater investigation, electrical and telecommunication/NBN connection investigation by the preferred consultant. 3. A further report be presented to Council in the first quarter of 2024 with an update on the budget, the findings of the investigations and the progression of the planning proposal. Harris/Medcalf	Preferred contractor advised of outcome of Council meeting. The consultant is currently working through final design changes and options paper before the matter can be presented back to Council.	August 2024
November 2023	DEP	**2023/276 17.5 GOANNA MANOR - LIONEL HUNT PARK, 125 BATHURST STREET, CONDOBOLIN** **RESOLVED THAT:** 1. The Acting Director of Environment, Tourism and Economic Development Report No. R23/261 be received and noted.	EOI developed for demolition and currently open. Public notice for stakeholder	September 2024

ACTIVE RESOLUTIONS AS AT 17 JULY 2024

		2. The condition of the building be noted, the premises remain vacant, and $60,000 from the current SRV building budget for 2023/2024 be allocated for the demolition of the building, including undertaking a historic and photographic record. 3. Stakeholder consultation be undertaken prior to the demolition of the building, subject to any regulatory requirements. 4. The Callara Cultural and Heritage Aboriginal Corporation be advised that the building is not available for their requested use. Harris/Medcalf	consultation was issued on 2 April 2024 and closed on 26 April 2024. Report on submissions received following public consultation presented to the May 2024 Council meeting. A further report was presented to the June 2024 Council meeting. A professional photographer attended the site on 1 July 2024. CCHAC have been advised that the building is not available for their requested use.	

ACTIVE RESOLUTIONS AS AT 17 JULY 2024

July 2023	DEP	**2023/175 17.5 WILLOW BEND SPORTS CENTRE IMPROVEMENTS** **RESOLVED THAT:** 1. The Director Environment, Tourism and Economic Development Report No. R23/195 be received and noted. 2. That Council proceed with Option 3 as outlined in this report. Harris/Mortimer	A variation request will be lodged for the LRCI grant as per Council's resolution. Purchase Orders have been placed for the cubicle works and flooring. Works schedule has been finalised with contractor for commencement by end of November. Operator has been notified of works schedule for amenities. The majority of works have been undertaken and finalisation is expected shortly.	August 2024

ACTIVE RESOLUTIONS AS AT 17 JULY 2024

July 2023	DEP	**2023/177 17.7.1 MCINNES STREET LAKE CARGELLIGO MASTER PLAN** **RESOLVED THAT:** 1. The Director of Environment, Tourism and Economic Development Report No. R23/211 be received and noted. 2. A planning proposal be prepared and lodged with Department of Planning and Environment to re-zone the site RU5 Village under Lachlan Local Environmental Plan 2013. 3. Detailed contamination and geotechnical soil investigations be undertaken by the preferred consultant. 4. A further $100,000 from the Housing and Development reserve be approved to continue investigations into 1 McInnes Street to determine the development potential of the site and prepare the preliminary design for the site. 5. A further report be presented to Council in the final quarter of 2023 with an update on the budget, the findings of the investigations and the progression of the planning proposal. Carter/Phillips	The Planning Proposal to re-zone the site to RU5-Village was lodged with the Department of Planning, Housing and Infrastructure (DPHI) in March 2024. Investigations have progressed and are now with Calare Civil. An update report will be provided once the consultants have completed some minor design changes. Gateway approval for the rezoning was received from DPHI on 12 April 2024. Agency consultation is currently underway (June 2024), followed by public consultation.	Ongoing

ACTIVE RESOLUTIONS AS AT 17 JULY 2024

May 2023	DEP	**2023/116 11.2 NOTICE OF MOTION - MEMORIAL TO DAVID DOYLE AND NEIL DUNNE** **RESOLVED THAT:** 1. Notice of Motion Report No. R23/115 be received and noted. 2. Council investigate and liaise with the families of the late David Doyle & Neil Dunne of D&D Technologies in honoring them for the life saving device they developed which has saved countless children's lives world-wide. 3. Council communicate with the Doyle and Dunne families and D&D Technologies to see what type of memorial they would prefer and determine if they will finance the memorial and support Council with this proposed project. Brady/Carter	Investigation/research is currently in progress.	December 2024
May 2023	DEP	**2023/127 17.6 CONSIDERATIONS IN THE FUTURE DELIVERY OF WASTE SERVICES FOR BURCHER RESIDENTS.** **RESOLVED THAT:** 1. The Director Environment Tourism and Economic Development Report No. R23/135 be received and noted. 2. Stakeholder consultation be undertaken regarding the future delivery of waste services in Burcher in accordance with a stakeholder consultation plan. 3. A further report be provided to Council, outlining stakeholder feedback and to seek a final decision from Council on the delivery of waste services in Burcher. Phillips/Bartholomew	Initial stakeholder consultation has been completed. Information collected during the consultation period is now being collated. Further public consultation is to be organised in the second half of 2024. Project has been added to funding list requested by Roy Butler MP for consideration in the State Budget.	December 2024

ACTIVE RESOLUTIONS AS AT 17 JULY 2024

July 2022	DEP	**2022/222 NSW FLOOD PLANNING PACKAGE** **RESOLVED THAT:** Council resolve to amend Lachlan DCP 2018 to include flood planning controls and mapping and that a further report be presented outlining the proposed changes before the draft DCP is placed on public exhibition. Harris/Bendall	The Draft DCP will be prepared subject to resource availability. Further flood studies are currently underway.	Ongoing
MAY 21	DEP	**92/2021 HONOUR ROLL/ACKNOWLEDGEMENT BOARD** **RESOLVED THAT:** That an Acknowledgement Board project be considered, along with other meritorious projects, for a funding application under the Stronger Country Communities Fund – Round 4. Subject to Council approval, and a successful grant application for the Acknowledgement Board project, expressions of interest be invited from community members to assist with the determination of appropriate criteria for a person's name to be considered for inclusion on the board. The advisory group is also to make recommendations to Council on the initial list of people's names for inclusion on the board. A further report be presented to Council following determination of the project funding application. Harris/Brady	The project was not supported by Council for funding under the Stronger Country Communities Fund – Round 4 or the LRCI4A funding programs. Other funding opportunities will now need to be identified. Subject to funding being received. No current grants match the proposal.	Ongoing
FEB 18	DEP	**28/18 LAKE CARGELLIGO WASTE FACILITY – LAND ACQUISTION** **RESOLVED THAT:** Approve the proposal to acquire 72,700 square metres of crown land comprising part lot 7308 DP 1151003, lot 7009 DP 1057453 and lots 7005 and 7006 DP: 1029763. Authorise the General Manager to lodge a Compulsory Acquisition Consent to Acquire Crown Land Application to the Department of Industry – Lands.	Now that the acquisition process is complete, an estimated cost will be determined for the construction of the access road for funding consideration. Further progress dependent on funding being allocated.	Ongoing

ACTIVE RESOLUTIONS AS AT 17 JULY 2024

		The DIS provide an estimated cost of the access road to the March Ordinary Council meeting. Phillips/Hall		
DEC 2017	DEP	**326/17 HERITAGE COMMITTEE MEETING 22 NOVEMBER 2017** **RESOLVED THAT:** Adopt the recommendations made by the Heritage Advisory Committee as follows; a) That Council implement a Conservation Management Plan for small rural cemeteries within the Shire. b) That Council award $6,000 to Meredith Ervin for works to the NAB and residence in Lake Cargelligo; $6,000 to Katrina & Jim Thomas for restoration works at Melrose Homestead, and $2,000 to the Tottenham & Albert Cemetery Committee for headstone restoration. Rees/ Frankel	Council's heritage advisor is currently focusing on assisting applicants for the new round of heritage grants. The new heritage grants funding round opened on 27 May 2024 and will be closing on 22 July 2024.	August 2024
June 2024	C&CS	**2024/135** **17.1 REQUEST FOR WATER ADJUSTMENT - ASSESSMENT NO. 1003715** **RESOLVED THAT:** 1. The Director of Corporate and Community Services Report R24/103 be received and noted. 2. Council approve a reduction of the water account for the 2024 period 2, of $3,097.05 which is calculated as per Council's Undetected Water Leak and Faulty Water Meter Policy. 3. The ratepayer be advised this is the first and only application allowable under the Undetected Water Leak and Faulty Water Meter Policy. **Brady/Bartholomew**	In progress	July 2024

ACTIVE RESOLUTIONS AS AT 17 JULY 2024

June 2024	C&CS	**2024/122 9.2.4 COMMUNITY DONATION AND EVENT SUPPORT PROGRAM** **RESOLVED THAT:** 1. The Director of Corporate and Community Services Report R24/140 be received and noted. 2. Council resolves to approve: (a) a donation of $500 to the Callara Culture & Heritage Aboriginal Corporation for the production of 2 books, on the proviso the books are published by 31 October 2024. This donation is to be funded from GL 3020.405 Elected Members general donations. (b) If the books are not published by this date, the funds are to be returned to council. 3. Council resolves to: (a) approve a donation of $200 for Skyfest 2024 from GL 3820.460 Community events and; (b) request the balance of the donation approved at the October 2023 meeting (resolution number 2023/241) amounting to $800 be refunded to Council, within 30 days. To be returned to GL 3820.460 Community events. 4. Council notes the donation of $500 approved at the May 2024 meeting (resolution 2024/97) to Lakes Alive/Lake Cargelligo Progress Association is for the ongoing beautification of Dead Man's Point, not Frogs Hollow. 5. Council resolves to transfer $7,000 from Elected members general donations GL 3020.405 to Special Events in kind support GL 230.509 Harris/Bartholomew	Correspondence issued and payment processed 21 June 24. Completed Correspondence issued 21 June 24. Refund will be made by mid July 2024 as per Nicole Smith phone conversation on 25 June 24 Correspondence issued and payment processed 21 June 24. Completed	COMPLETED IN PROGRESS – August 2024 COMPLETED

ACTIVE RESOLUTIONS AS AT 17 JULY 2024

May 2024	C&CS	**2024/113 18 APPOINTMENT OF INDEPENDENT FACILITATOR TO REVIEW THE ARIC CHAIRPERSON, REVIEW OF INTERNAL AUDIT EFFECTIVENESS AND REVIEW OF ARIC EFFECTIVENESS** **RESOVLED THAT:** 1. The Director Corporate & Community Services Report R24/130 be received and noted. 2. Council resolves to appoint GHR Accounting to undertake the review of the ARIC Chairperson. 3. Council resolves to appoint Mead Perry to undertake the review of the ARIC. 4. Council resolves to appoint Centium to undertake the review of the Internal Audit. Brady/Harris	All companies have been notified of their appointment. Meetings have been held with DCCS and other relevant individuals. All required participants have been notified. ARIC Chair Performance review submitted to June 2024 meeting. August 2024-Internal Audit & ARIC effectiveness. Completed & included in the July 2024 council meeting reports. Completed	COMPLETED
May 2024	C&CS	**2024/101 9.2.5 REVIEW OF THE COMMUNITY DONATION AND EVENT SUPPORT POLICY** **RESOLVED THAT:** 1. The Director of Corporate & Community Services Report R24/108 be received and noted. 2. The Community Donation and Event Support Policy v2 be adopted, as presented, with effect from 1 July 2024. 3. Council delegates to the General Manager, with the approval of the Mayor, the power to grant financial assistance under section 377(1A) of the *Local Government Act 1993.* 4. Council rescinds all and any prior resolutions for community event support, donations, fee concessions, and rates and charges	Policy published on the website Associated policy documents updated and published on the website - Complete	COMPLETED

ACTIVE RESOLUTIONS AS AT 17 JULY 2024

		donations, unless specifically listed in the Integrated Planning and Reporting documents commencing 1 July 2024. 5. Council rescinds the Community Donation & Event Support Policy v1 that was last adopted June 2023, and any donations policies that may have not already been previously extinguished. Harris/Bartholomew		
May 2024	C&CS	**2024/93 9.2.4 COMMUNITY DONATION AND EVENT SUPPORT PROGRAM - FUNDING ROUND APPLICATIONS** **RESOLVED THAT:** 1. The Director of Corporate and Community Services Report R24/105 be received and noted. 2. Council rescinds Resolution 2024/57 for the Tullibigeal Team Penning as the event has been cancelled due to lack of entries. An estimated amount of $400 for in-kind support was approved at the March 2024 Council Meeting. 3. Council approves the transfer of $3,000 from the elected member general donation to the in kind support budget. 4. Council approve a financial donation of $500 for Dance 2873. This donation will be funded from the Annual Budget for Elected Members General Donation, and is conditional on the event proceeding. 5. Council decline the application from the Lachlan Arts Council – Film Footage project and invite them to submit another application in the future. 6. Council approve the request from the Lachlan Arts Council to retain the $500 funding for the "tile project". This financial donation was funded from the annual budget for general donation - elected members and is conditional on the project completing by 31 august 2024. Harris/Blewitt	completed completed Correspondence issued 22 May 2024. Payment processed 19 June 24 - Completed Correspondence issued 22 May 2024 - Completed Correspondence issued 22 May 2024 – Completed	COMPLETED

ACTIVE RESOLUTIONS AS AT 17 JULY 2024

May 2024	C&CS	**2024/94 9.2.4 COMMUNITY DONATION AND EVENT SUPPORT PROGRAM - FUNDING ROUND APPLICATIONS** **RESOLVED THAT:** 7. Council approves a financial donation of $500 to Can Assist for their High Tea event. This donation will be funded from the Annual Budget for General Donation– Elected Members and is conditional on the event proceeding. Blewitt/Brady	Correspondence issued 22 May 2024. Payment processed 14 June 24 - Complete	COMPLETED
May 2024	C&CS	**2024/96 9.2.4 COMMUNITY DONATION AND EVENT SUPPORT PROGRAM - FUNDING ROUND APPLICATIONS** **RESOLVED THAT:** 9. Council agree that Community Donation and Event Support Program Funding Round Applications – Item number 9 be deferred until the next meeting of Council scheduled to be held on 19 June 2024. Blewitt/Harris	Council resolved at the June meeting to provide $500 to Callara. Correspondence issued and payment processed 21 June 24. Completed	COMPLETED
May 2024	C&CS	**2024/97 9.2.4 COMMUNITY DONATION AND EVENT SUPPORT PROGRAM - FUNDING ROUND APPLICATIONS** **RESOLVED THAT:** 10. Council decline the request for a financial donation of $1,200 from the Condobolin Public School P&C for their "Get Arty" project, as this is not permitted under the policy. 11. Council approve a financial donation of $300 for the Condobolin RSL Diggers Swimming Club on the proviso the club continues to hold the "Diggers weekly swims". This financial donation is to be funded from the Annual Budget for Elected members General Donation. 12. Council approves a donation of $500 to Lakes Alive/ Lake Cargelligo Progress Association for the ongoing beautification of Frog's Hollow. This financial donation will be funded from the	Correspondence issued 24 May 24-completed Correspondence issued 24 May 24. Payment processed 14 June 2024. Completed Correspondence issued 24 May 24. Payment	COMPLETED

ACTIVE RESOLUTIONS AS AT 17 JULY 2024

		Annual Budget for Elected Members General Donation and is conditional on the group continuing with beautification activities. 13. Council approve the request from the Condobolin PAH & I Association for in-kind support, estimated to be worth $15,250 for the show. This contribution is to be funded from the In-Kind support budget and is conditional on the show proceeding. 14. Council approve the request from the Condobolin Camp Draft Association for a financial donation of $500 and in-kind support of estimated worth $3,430. This contribution is to be funded from the In-Kind contributions budget. This is conditional on the event proceeding. 15. Council approve a financial donation of $800 for the Tottenham Hospital Auxiliary Branch to support their Annual Spring Fair Luncheon. This financial donation will be funded from the Annual Budget for General Donation – Elected Members and is conditional on the event proceeding. Harris/Blewitt	processed 14 June 2024. Completed Correspondence issued 24 May 24. Completed Correspondence issued 24 May 24. Payment processed 19 June 24 – Completed Correspondence issued 24 May 24. Payment processed 18 June 24 – Completed	COMPLETED
May 2024	C&CS	**2024/99 9.2.4 COMMUNITY DONATION AND EVENT SUPPORT PROGRAM - FUNDING ROUND APPLICATIONS** **RESOLVED THAT:** 17. Council approve a financial donation of $800 for the Born to Read Condobolin event.This financial donation will be funded from the Annual Budget for Elected Members General Donation, and is conditional on the event proceeding. Brady/Mortimer	Correspondence issued 22 May 2024. Payment processed 25 June 24 - Completed	COMPLETED
May 2024	C&CS	**2024/100 9.2.4 COMMUNITY DONATION AND EVENT SUPPORT PROGRAM - FUNDING ROUND APPLICATIONS** **RESOLVED THAT:** 18. Council approves a financial donation of $4,095.39 to the Condobolin & District Kennel Club Incorporated to cover the cost of mobile lighting towers. This donation is to be funded from the	Correspondence issued 22 May 2024. Payment processed 14 June 24 - Completed	COMPLETED

ACTIVE RESOLUTIONS AS AT 17 JULY 2024

		Community Events program budget and is conditional on the All Breeds Championship Dog Shows event proceeding. 19. Council approve in kind support of an estimated $5,980 for the Lake Cargelligo Show. This contribution is to be funded from the In-Kind contributions budget and is conditional on the show proceeding. Harris/Blewitt	Correspondence issued 24 May 24. Completed	
May 2024	C&CA	**2024/92 9.2.3 MODERN SLAVERY POLICY V1** **RESOLVED THAT:** 1. The Director Corporate and Community Services Report R24/38 be received and noted. 2. The Draft Modern Slavery Policy v1 be placed on public exhibition for 28 days, and adopted subject to no significant responses being received. Brady/Harris	Modern Slavery Policy Published on website no submissions were received - COMPLETED	COMPLETED
May 2024	C&CS	**2024/91 9.2.2 PUBLIC INTEREST DISCLOSURE POLICY** **RESOLVED THAT:** 1. The Director Corporate and Community Services Report R24/40 be received and noted; 2. The draft Public Interest Disclosure Policy be placed on public exhibition for 28 days, and adopted subject to no significant issues being raised. 3. Council rescinds the Internal Report Policy adopted April 2020 and all earlier versions. 4. Council rescinds all earlier versions of the Public Interest Disclosure Policy. Harris/Bartholomew	In progress. Public Interest Disclosure Policy on public exhibition. With a closing date of 16 July 24	August 2024

ACTIVE RESOLUTIONS AS AT 17 JULY 2024

May 2024	C&CS	**2024/90 9.2.1 DRAFT INTEGRATED PLANNING & REPORTING DOCUMENTS 2024.2025** **RESOLVED THAT:** 1. The Director Corporate and Community Services Report R23/380 be received and noted. 2. The draft Operational Plan 2024-2025, the 2022-2026 Delivery Program, the draft updated Resourcing Strategy, the draft Fees and Charges, and the 10 year Long Term Financial Plan be placed on public exhibition for a period of 28 days from 16 May to 13 June 2024. 3. Following the completion of the public exhibition period the Director of Corporate and Community Services present a further report, summarising any submissions received during the public exhibition period, for the consideration of Council prior to final adoption of the Operational Plan (OP) 2024-2025, the 2022-2026 Delivery Program, the updated Resourcing Strategy, the draft Fees and Charges, and the Long Term Financial Plan. Harris/Mortimer	Completed. Budget adopted in June 24.	Completed
June 2024	IS	**2024/144 17.10 SUPPLY AND DELIVERY OF ONE NEW 4X2 TRUCK** **RESOVLED THAT:** 1. The Director Infrastructure Services Report R24/183 be received and noted. 2. The offer from Wagga Trucks for the supply of one new Hino 721AT4400 with lifting crane be accepted and fleet number 7028 be sold at Pickles Auctions as per (options 1). 3. Council approve the necessary fund transfers from the Plant Reserve to the Plant Replacement Capital Works Program – Truck Replacement. **Harris/Medcalf**	Purchase order issued.	Complete

ACTIVE RESOLUTIONS AS AT 17 JULY 2024

June 2024	IS	**2024/143 17.9 SUPPLY AND DELIVERY OF ONE NEW 4X4 TRUCK** **RESOVLED THAT:** 1. The Director Infrastructure Services Report R24/181 be received and noted. 2. The offer from Wagga Trucks for the supply of one new Hino 817 Med 4x4 Crew Cab with super single wheels & tyres and their trade offer for fleet number 7025 as per options 1 be accepted. 3. Council approve the necessary fund transfers from the Plant Reserve to the Plant Replacement Capital Works Program – Truck Replacement. **Brady/Harris**	Purchase order issued.	Complete
June 2024	IS	**2024/141 17.7 TENDER ASSESSMENT - T2023/16 CONDOBOLIN BOREFIELDS II SCHEME - CONTRACT NO.3: CONDOBOLIN WTP MODIFICATIONS** **RESOLVED THAT:** 1. The Director Infrastructure Services Report No. R24/168 be received and noted. 2. Council resolve to decline to accept any of the tenders submitted in response to the T2023/16 Condobolin Borefields II Scheme – Contract No.3: Condobolin WTP Modifications. 3. Council authorise the General Manager or their delegate to enter into direct negotiations with Trazlbat Pty Ltd with a view to entering into a contract in relation to the subject matter of the RFT. 4. Council note that the reason for entering into direct negotiations is that it is not expected that further market testing will provide a more satisfactory result. 5. Following the completion of further negotiations, the Director of Infrastructure Services present a further report for Council's consideration. **Harris/Bartholomew**	See Council Report	Complete

ACTIVE RESOLUTIONS AS AT 17 JULY 2024

April 2024	IS	**70/2024 9.4.2 PART ROAD CLOSURE - LACHLAN VALLEY WAY, FAIRHOLME** **RESOLVED THAT:** 1. The Director Infrastructure Services Report No. R24/102 be received and all feedback from the consultation be noted. 2. Council resolve to close that part of MR 377 Lachlan Valley Way, Fairholme, as identified in the report. 3. Council authorise the Mayor and General Manager to execute the necessary documents and affix the Council seal. Harris/Mortimer	Completed	complete
March 2024	IS	**2024/44 9.4.2 CROWN RESERVE 96552 AND 96536 LAKE CARGELLIGO** **RESOVLED THAT:** 1. The Director Infrastructure Services Report No. R24/70 be received and noted. 2. Council acknowledge that Crown Reserve 96552 will be devolved to Council once the Lake Cargelligo Sport Club Ltd ceases to be the Crown Land Manager. 3. Council write to Department of Planning Housing & Infrastructure - Crown Lands and discuss possible future options for the Management of Crown Reserve 96536. Harris/Brady	See Council Report	Complete

ACTIVE RESOLUTIONS AS AT 17 JULY 2024

March 2024	IS	**2024/43 9.4.1 HOLT STREET DRAINAGE - CONSULTATION UPDATE** **RESOVLED THAT:** 1. The Director Infrastructure Services Report No. R24/69 be received and noted. 2. Council continue discussions with land owners of Lot 3 Section 26 DP 75859 and Lot 4 Section 24 DP 758595 with the intention of formalising an additional drainage easement adjacent to the current drainage easement. 3. Council prepare detailed design drawings and cost estimate for drainage upgrade on the concrete trapezoidal drain option. Mortimer/Medcalf	Consultant engaged to confirm detailed design	August 2024
November 2023	IS	**2023/280 17.9 CONTRACTS FOR THE SUPPLY AND DELIVERY OF ROAD SIGNS** **RESOLVED THAT:** 1. The Director Infrastructure Services Report No. R23/323 be received and noted 2. Contracts for the supply and delivery of road signs from the following suppliers be accepted: (a) Artcraft, (b) Barrier Signs, (c) DeNeefe Signs and (d) Hi-Vis Group 3. The General Manager be authorised to sign the contract documents and affix the Council seal. Harris/Medcalf	Contract documents sent for execution. Awaiting response	August 2024

ACTIVE RESOLUTIONS AS AT 17 JULY 2024

March 2023	IS	**2023/49 9.4.1 ROAD ENCROACHMENT ORANGE STREET, CONDOBOLIN** **RESOLVED THAT:** 1. The Director Infrastructure Services Report No. R23/62 be received and noted. 2. The Council acquire part of Lot 3, Sec A, DP 16964 pursuant to section 177 of the Roads Act 1993 for the purpose of road widening at the intersection of Orange, Tasker and Fay Streets, Condobolin. 3. The Council will acquire the Land by compulsory process pursuant to section 30 of the Land Acquisition (Just Terms Compensation) Act 1991. 4. The Council instructs its solicitors to make application to the Minister of Local Government to approve the acquisition under the Land Acquisition (Just Terms Compensation) Act 1991. Brady / Rees	Solicitor has been advised and requested to progress the matter.	August 2024.
February 2023	IS	**2023/26 17.5 LAND ACQUISITION - LACHLAN VALLEY WAY FOR ROAD WIDENING AND CONDOBOLIN BORE FIELDS** **RESOLVED THAT:** 1. The General Manager's Report No R23/38 be received and noted. 2. Council note the conditions of the draft Deed of Agreement for the Acquisition of Land and Grant of Easement and Water Use. 3. Council authorise General Manager to negotiate and accept any minor variations to the agreement requested by the landowner that do not materially change the agreement. 4. The Mayor and General Manager be authorised to sign the Deed of Agreement for the Acquisition of Land and Grant of Easement and Water Use upon acceptance by the landowner.	Complete	Complete

ACTIVE RESOLUTIONS AS AT 17 JULY 2024

		5. Upon signing the Deed of Agreement Council acquire the land shown as New Road Land in Schedule 2 of the Deed of Agreement under the Land Acquisition (Just Terms Compensation) Act 1991 (NSW). 6. Upon signing the Deed of Agreement Council close and transfer the redundant road reserve shown as Verge Land in Schedule 2 of the Deed of Agreement to the landowner under Section 44 of the Roads Act 1993. 7. The Mayor and General Manager be authorised to sign all necessary documents, applications and plans associated with the acquisition, closure, transfer and registration of the land matters contemplated in this report and affix the Council seal as necessary. Phillips/Mortimer		
OCT 21	IS	**243/2021 FY21/22 UTILITIES MONTHLY UPDATE FOR SEPTEMBER** **RESOLVED THAT:** Refer the RNSW842 Sewage Effluent Reuse Management System project costings for Tottenham to the Project Steering Committee for further discussion, highlighting the high ongoing cost for the proposed system. Harris/Hall	Public Expression of Interest process to be undertaken to identify potential users	August 2024.
JUNE 21	IS	**147/2021 BURCHER WATER TREATMENT UPDATE** **RESOLVED THAT:** The outcomes from the stakeholder information session held on 1 June 2021 be noted. Council provide guidance on the matter of water supply for the community of Burcher. Harris/Bendall	Ongoing.	Ongoing.

CENTRAL NSW JOINT ORGANISATION

Report: Modern Slavery Risk Assessment Project Update

Recommendation:

That Council note the Central NSW Joint Organisation Modern Slavery Report and participate in ongoing collaboration across the region to minimise duplication and reduce regulatory burden.

Background

Council will recall the Modern Slavery Risk Assessment Project is being progressed through the CNSWJO and participating members. Please find the previous report to Council attached.

The NSW Modern Slavery Amendment Act, 2021 requires local government to take reasonable steps to ensure that goods and services procured by and for Council are not the product of modern slavery.

Guidance on reasonable steps was provided in December 2023 please find more detail in its regard in a table below. Arguably this Guidance is onerous and impractical.

CNSWJO is keen to provide as much support and advice as possible with a view to ensuring Council does not duplicate effort and is aware of the policy position of the CNSWJO Board regarding Modern Slavery.

Policy advice

Where efforts to counteract slavery are laudable, they must be practical and

Case Study – Modern Slavery Legislation – how an under resourced State entity drives costs up for Local Government and their suppliers.

Everyone supports the idea of fighting modern slavery through better supply chains. How should this be implemented?

As it stands, councils must manage the modern slavery risks of their supply chains including international businesses. Every council, every supply chain. Councils must report their compliance in a formal Annual Report to the Auditor General, annually online with the Anti-Slavery Commission and as from 1 July 2025 Online Reporting to the Anti-Slavery Commission for all contracts arising from any high-risk procurement with a value of $150K within 45 days from the date of contract.

Suppliers deemed high risk must be surveyed. Surveys alone are not enough; councils must also demonstrate due diligence and show what they are doing to reduce the risks including following up non respondents and offering them support in lowering their risks. All suppliers must be informed of their ratings. The total list of suppliers for Bathurst Regional Counil is approximately 4,000, with over 100 currently rated as high risk. The estimate for the CNSWJO region's members is 14,600, with a lot of overlap.

Meanwhile the advice on the Federal Attorney General's website is that though they have a Register for Modern Slavery they do not check the veracity of the advice therein. Checking become councils' job. The Commissioner suggests that this could include contacting business directly – hopefully councils have staff fluent in the languages of those countries viewed as high risk.

To be compliant, legal advice directed there be 14 questions on Modern Slavery in every procurement activity the CNSWJO undertakes. Every supplier responding to Requests for Quotation and Tender must respond to these questions. The Commissioner's guidance is suggesting these questions should be weighted between 5-10%. This competes with other criteria like safety, capability, quality, environmental, pricing and supporting local providers.

CNSWJO is undertaking this work collaboratively to try and reduce duplication both for suppliers and councils and can report that suppliers are furious.

Case Study: Modern Slavery Legislatio

achievable. The current guidance from the Office of the Anti-slavery Commissioner is neither practical nor achievable, rather it reflects a poor understanding of Councils and their suppliers.

Modern Slavery Legislation has not considered the resourcing impacts on local government and is yet another cost shift from a poorly resourced regulator.

The CNSWJO Board has been using the Case Study on Modern Slavery on the cover page of this report for advocacy purposes where on the one hand both the NSW Government generates resource intensive cost shifts like compliance with this legislation, then rate caps and finally conducts an inquiry in local government financial sustainability – all in a less than six months.

Operational Program support

CNSWJO is of a view that the work it is undertaking drives a sensible pathway supporting the objectives of the modern slavery legislation.

A central database has been developed using information on suppliers provided by member councils. The database identifies medium and high-risk suppliers, who then receive a survey link requesting information about their modern slavery policies, reports, training and communication. In December, the survey was sent to over 300 suppliers who had until 29 February 2024 to respond with the requested information. Responses were received from 45 suppliers.

Work is now underway to collect information from Local Government Procurement (LGP) who has also conducted a similar risk assessment on many of the same suppliers. Prior to the survey being sent again, CNSWJO will ensure that any information already collected via LGP is incorporated into the database to avoid duplication.

CNSWJO staff are working closely with Ms Donna Eastburn from Bathurst Regional Council who has provided a great deal of guidance to the risk assessment project. Advice is also being sought from LGP through their Sustainable Choice program.

Further, in December 2023, the Office of the Anti-slavery Commissioner released Guidance on Reasonable Steps to Manage Modern Slavery Risks in Operations and Supply Chains. While CNSWJO staff are reviewing the guidance and determining how to best support member councils, the following table sets out the implementation milestones of the Guidance for Reasonable Steps:

Date	*Milestone*
1 January 2024	*Guidance takes effect*
Contracts pre-dating 1 January 2024	***Do contracts need to be renegotiated?*** *There is no general expectation that contracts or agreements pre-dating this Guidance will be re-negotiated.* • *Exceptionally, where modern slavery risks in an ongoing operational activity or procurement are Heightened, covered entities must not only use leverage but also develop it where they lack it. This is consistent with Australia's commitment to the UN Guiding Principles on Business and Human Rights and recent adherence to the OECD Council Recommendation on the Role of Government in Promoting Responsible Business Conduct. In some cases, especially where there is a salient risk of ongoing modern slavery in the performance of the*

	contract, this could mean that entities do need to consider exploring contractual adjustments in order to develop this leverage. ***What steps are reasonable where earlier contracts are still on foot?*** *Where a contract pre-dates 1 January 2024 but remains on foot, reasonable steps may be required – for example in relation to contract management. This may necessitate an assessment of the GRS due diligence level associated with a contract already entered into, and still on foot – see Part 4.* • *Contract management may require using existing forms of leverage, such as contractual obligations to abide by workplace health and safety standards (locked accommodation, excessive working hours, abusive behaviour). Some procurement contracts or agreements may already include references to ISO 45001 Occupational Health and Safety Management Systems, ISO 26000 Social Responsibility, or ISO 20400 Sustainable Procurement.* • *Ongoing contracts may also activate expectations under this Guidance relating to supplier capability development, grievance mechanisms and remediation.*
	Do entities have to report on activities and procurement prior to 1 January 2024? *Many covered entities had obligations to take reasonable steps that commenced on 1 July 2022. They must report on the reasonable steps they have taken since that time. (See Appendix K GRS Annual Reporting Template.) While the Guidance only takes effect from 1 January 2024, it may provide inspiration for reporting on earlier activity. Further clarifications about reporting expectations are set out below, with reference to when reporting takes place.*
Reporting between 1 January 2024 and 30 June 2024	*Entities reporting in 2024 on activity undertaken from 1 January 2023 to 31 December 2023 need only use the Guidance as inspiration. They are however still expected to report using the provided template and online form. In monitoring this reporting, the Commissioner will take into account that the Guidance was not available until December 2023 and only takes effect on 1 January 2024.*
1 July 2025	*Transactional reporting obligations relating to heightened modern slavery due diligence (**HMSDD**) procurements commence. Entities should file an online report with the Office of the Anti-slavery Commissioner within 45 days of the entry into force of any contract:* • *arising from a 'Heightened' modern slavery due diligence procurement process; and* • *with a value of AU $150,000 (including GST) or more. For more detail see Appendix L Heightened MSDD reporting.*
Annual reporting occurring between 1 July 2024 and 31 December 2024	*Entities reporting on activity undertaken from 1 July 2023 to 30 June 2024 should endeavour to report against the Guidance for the full year of activities – see Part 6. These entities may find it necessary to assess the GRS due diligence level associated with transactions that took place before 1 January 2024, in order to meet the annual reporting obligations set out in this Guidance. In monitoring this reporting, the Commissioner will take into account that the Guidance was not available until December 2023 and only takes effect on 1 January 2024.* *In reviewing this reporting, the Anti-slavery Commissioner will focus in particular on:*

	1. *conformance with Part 1 of this Guidance;* 2. *Heightened MSDD contexts;* 3. *procurement related to* ***— information and communication technologies (ICT)*** ***— cleaning services.***
Annual reporting occurring between 1 January 2025 and 31 December 2025	*Guidance in effect. Covered entities expected to make best efforts to conform with all aspects of this Guidance. In reviewing this reporting in 2025, the Anti-slavery Commissioner will pay attention to:* 4. *Heightened MSDD contexts;* 5. *procurement related to* *— information and communication technologies (ICT)* *— cleaning services* *— **renewable energy** and* *— **domestically produced food and agriculture***
Annual reporting between 1 January 2026 and 31 December 2026	*Guidance in effect. Covered entities expected to make best efforts to conform with the Guidance. In reviewing this reporting in 2026, the Anti-slavery Commissioner will pay attention to:* • *modern slavery risk management in Heightened MSDD contexts;* • *procurement related to* *— information and communication technologies (ICT)* *— cleaning services* *— renewable energy* *— domestically produced food and agriculture and* *— **construction**.*

Where the resourcing required by councils to demonstrate compliance with the requirements outlined above is burdensome, General Managers of the region have proposed that a meeting be coordinated to determine the progress each council is making as well as to determine what further support is required. This is being progressed.

Conclusion

Modern Slavery Legislation has generated significant resourcing impacts for Councils. The CNSWJO is both advocating and providing operational support for Council to help minimise these impacts.

Value for Council

The work on Modern Slavery being undertaken by the CNSWJO is part of the regional Best Practice in Aggregated Procurement Program. The Toolkit for this program was fully funded by the NSW Government and its implementation comes at no extra cost to Council outside membership fees to the JO.

The return on investment from the fees Council contributes to the JO for the 2022/2023 year was 9.4:1. This is primarily for cost savings on aggregated procurement and grant funding.

Attachment: Previous report provided to Councils in November 2023

Recommendation: That Council note the progress of the regional modern slavery compliance project supported by CNSWJO.

Introduction

The NSW Modern Slavery Amendment Act, 2021 requires all Local Government Sites to take reasonable steps to ensure that goods and services procured by and for Council are not the product of modern slavery.

Modern Slavery is defined as the severe exploitation of other people for personal or commercial gain. It is estimated that globally 50 million people are trapped in modern slavery. It has been identified that there are around 41,000 potential victims in Australia.

Modern slavery comes in many forms. The most common forms are:

- Human trafficking – involves transporting, recruiting, or harbouring people for the purpose of exploitation, using violence, intimidation, threats or coercion.
- Forced labour – any work or services which people are forced to do against their will under the threat of some form of punishment this includes debt bondage, child slavery and servitude.

Slavery exists in all stages of the supply chain, from the picking of raw materials to the manufacturing of goods and at the later stages of shipping and delivery to consumers.

Background

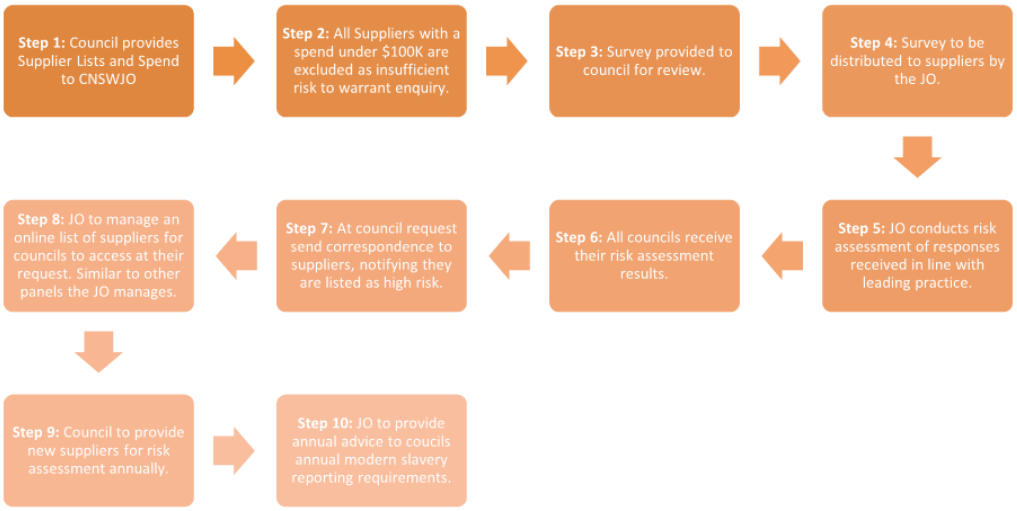
CNSWJO, at the request of members is developing a regional approach to compliance that is:

- offering efficiencies and reducing council resource required;
- managing an ongoing supplier risk assessment; and
- the one point of contact for suppliers for councils in the region to minimise the extent to which businesses need to respond to the modern slavery risk assessment process.

Project Objectives: This project serves to provide CJSWJO, its member and associate member councils that the suppliers they are engaged with are not providing goods and services that are the product of modern slavery, and it will allow an assessment of all the suppliers across councils. It will require suppliers to demonstrate their compliance with the regulations and ensure they are thinking about modern slavery and implementing practices and policies in their workplace to avoid inappropriate workplace practices.

Project Deliverables: This project will consist of a survey distributed to the member council's suppliers. CNSWJO will facilitate an evaluation detailing each supplier's risk rating.

Flow Chart



Efficiencies and other value to councils

A regional approach to modern slavery will enable efficiencies by shifting the focus from an individual council process to a regional collaborative effort to understand the region's suppliers and conduct assessments from a regional point through the Joint Organisation. Completing this assessing work through the Joint Organisation will lessen the burden on suppliers who are utilised across councils throughout the region in responding to multiple surveys requesting the same or similar information. This work will result in a central data list that will be accessible for informational purposes to councils.

Council resources will still be required, as outlined in the above flow chart, in annually updating supplier lists and in keeping data accurate and up to date; however, councils will not be required to conduct the risk assessment each year, as this task will fall upon the Joint Organisation. With this process being an annual task, councils will then be able to report as required on the progress and status of keeping up to date with modern slavery legislation and taking a proactive stance in addressing modern slavery in their supply chains.

Manage an ongoing supplier risk assessment

The Joint Organisation will manage an ongoing/ annual supplier risk assessment as per the flow chart provided above. The steps taken will allow the Joint Organisation and member councils to keep track of suppliers utilised throughout the region and their risk levels concerning modern slavery.

The Joint Organisation, at the discretion of member councils, will advise suppliers of their risk rating when it exceeds a low rating. Any supplier with a medium to high-risk rating will be advised by the Joint Organisation of this rating and offered support to reduce their risk or modern slavery practices in their supply chains, where possible.

One point of contact for suppliers for councils in region to minimise the extent to which businesses need to respond to the modern slavery risk assessment process.

The new modern slavery regulations are applicable across the board for Organisations with a supply chain, if each individual organisation or council were to approach these requirements individually the number of surveys being distributed for completion would be excessive. Particularly throughout regions such as Central NSW where councils in utalise the same or similar suppliers for the provision

of goods and services. When factoring this in, it is optimal for the surveying to be completed through one point of contact to minimise the duplication and work required of the regions suppliers.

Financial and resourcing impacts
CNSWJO will manage the process including costs of surveys and the evaluation of the surveys.

No costs are anticipated to councils at this time.

Risk Assessment Evaluation Criteria
Collaboration with Bathurst Regional Council has informed the following risk evaluation process.

The criteria used in evaluating a supplier's modern slavery risk rating will include:

- Council spend with a supplier over $100K (annual spend below $100K is considered minor and will therefore be allocated a low rating);
- Modern Slavery Ratings List; and
- Country of origin in supply chain.

CATEGORY	OCCUPATIONS	RATING
ARTISTS	ARTISTS, PERFORMERS, BANDS, WRITERS, SPEAKERS,MCEE	LOW
CONSULTANTS	ARCHITECTS, PLANNERS, HERITAGE CONSULTANTS, INSPECTORS, SURVEYORS, DOCTORS, SOLICITORS,VALUERS	LOW
EMPLOYMENT	EMPLOYMENT, LABOUR HIRE, STAFF	LOW
FINANCIAL	AUDITORS, FINANCIAL CONSULTANTS, ACCOUNTANTS, SOLICITORS, BANKS, INSURANCE	LOW
FOOD	RESTAURANTS, FOOD VENDORS, JAMS AND PICKLES, CATERERS	LOW
GOVT	LOCAL, FEDERAL & STATE GOVERNMENT, LGP, TENDERLINK, AUST POST, INDUSTRY STANDARDS, LEGISLATION, ATO	LOW
HIRE	VENUE HIRE, EQUIPMENT HIRE, LEASES, STAGES ETC	LOW
LANDSCAPING	ARBORISTS, MOWING, MAINTENANCE, LANDSCAPERS, PLANTS, FLORISTS, GRAVEL	LOW
MEDIA	MAGAZINES, NEWSPAPERS, INFLUENCERS, TV, RADIO, SUBSCRIPTIONS, PHOTOGRAPHERS, MARKETING, PRINTING, WEB DESIGN	LOW
MEMBERSHIP	ASSOCIATIONS, BOARDS, SOCIETIES, SUBSCRIPTIONS, LICENCES, BUY LOCAL	LOW
MUSEUMS	ART GALLERIES, MUSEUMS, LIBRARIES, BOOKS	LOW
SOFTWARE	SOFTWARE, INTERNET, SUBSCRIPTIONS AND LICENCES, LINE RENTAL	LOW
TRAINERS	TRAINERS, CONFERENCES, WORKSHOPS, SEMINARS, WEBINARS	LOW
EVENTS	MAJOR HIRE OF PRODUCTS IE FERRIS WHEEL, ICE RINK	MED
SERVICES	PERFORMING A SERVICE IE PLANT HIRE, EQUIPMENT SERVICES, INSPECTIONS, CALIBRATIONS, PAINTERS, TRANSPORT & FREIGHT COMPANIES, DELIVERY SERVICES	MED
CHEMICALS	CLEANING COMPANIES, CHEMICAL COMPANIES, GAS, FUEL, ADDITIVES, ASBESTOS,	HIGH

CLOTHING	UNIFORMS, PPE	HIGH
CONSTRUCTION	MATERIALS USED FOR ANY BUILDING OR CONSTRUCTION INCLUDING PLUMBERS AND ELECTRICIANS; MACHINERY PURCHASES OR REPAIRS	HIGH
ENERGY	ENERGY COMPANIES, SOLAR PANELS AND LITHIUM BATTERIES	HIGH
HARDWARE	COMPUTER HARDWARE, CABLES ETC, PHONES, TABLETS	HIGH
MISC PRODUCTS	MUSEUMS STOCK, MISC PRODUCTS, ONE OFFS, SUPERMARKETS, SOUVENIERS, FURNITURE, ELECTRICAL ITEMS, SECURITY	HIGH
VEHICLES	CAR, TRUCKS, TRAILERS, LAWNMOWERS & OTHER EQUIPMENT INCLUDING ALL PARTS & SERVICES	HIGH
OTHER	CASE BY CASE TO BE DETERMINED: OVERSEAS PRODUCTS	TBA

REMOVED FROM LIST	EMERGENCY SERVICES, FUNDING, GRANTS, DONTATIONS, SPONSORSHIP, SCHOOLS UNIVERSITIES AND ALL GOVERNMENT DEPARTMENT DEPARTMENTS.	

Evaluation of High-Risk Respondents

Once suppliers have responded to the surveying, they will receive a risk rating.

Low risk countries/regions - Australia, New Zealand, UK, Canada, Europe

Medium risk countries - Malaysia, Mexico, Nepal, Philippines, Singapore, Sri Lanka, Thailand

High risk countries/regions - North Korea, Eritrea, Mauritania, Saudi Arabia, Türkiye, Tajikistan, United Arab Emirates, Russia, Afghanistan, Kuwait, India, China, North Korea, Pakistan, Russia, Indonesia, Nigeria, Türkiye, Bangladesh, United States

Conclusion

This project anticipates completion by 30 June 2024 with ongoing support provided to councils. The report is provided for noting.

Attachment/s: Nil

LACHLAN SHIRE COUNCIL

Community Donation and Event Support Policy

FUNDING APPLICATION FORM

LACHLAN SHIRE COUNCIL

Please read the policy carefully before completing this application form, as applications that do not meet the stated funding criteria may be deemed ineligible. Should you require assistance or advice in completing the application form, please contact Council on (02) 6895 1900.

PART A - Applicant Details

Name of group/organisation:
Condobolin Auto Sports Club

Postal Address:
2159 Boona Rd Condobolin NSW 2877

Contact Person:
James Patton

Position in group\organisation:

Telephone/Mobile:
0428962914

Email Address
Jamespatton24@gmail.com

Is your organisation incorporated? INC 9884350 (Yes) No

Does your organisation have an ABN? (Yes) ~~No~~

ABN
30 749 214 342

Does your organisation have Public Liability Insurance? (Yes) No

If yes, please attach a valid Certificate of Currency.

PART B - Project Details

Project Title:
Yellow Mountain Cross Country 2024

Project Location:
Tottenham to Condobolin and return

Proposed Start Date:
2 August 2024

Proposed End Date:
4 August 2024

Summary of Project:
The Yellow Mountain Cross Country is a two-day event consisting of approximately 240km each day. Racing between the townships of Tottenham and Condobolin in western NSW, it is run as an Interclub between the two MNSW Motorcycle clubs of Tottenham and Condobolin. The track is marked by arrows and the terrain consists of open red soil plains to snotty mallee trails to rocky hills.

Briefly summarise what your organisation does i.e. its mission.
as above.

How will this project benefit the local community?

National offroad event bring people to to Shire. Condobolin & Tottenham.

Please estimate the number of participants and/or spectators in your project.

Approximately 400 people

How will the success of the project be evaluated by your organisation?

Numbes of people
- everyone here & back safely.
Profit

How will your organisation acknowledge the financial contribution from Council?

Banners showing support from Council
Commitee will advertize.

Please outline how your organisation will manage this project.

Condobolin Auto Sports Club has monthly committee meetings to manage this event. This includes.....
job lists that give to people & ticked off by a due date.

PART C - Funding Sources

Has your organisation received funding assistance from Council before? ☑ Yes ☐ No

If Yes, in which financial year did your organisation last receive funding: 2023.

Please provide details of any funding sought from other sources for this project.

Funding Source	Amount	Secured (Yes or No)
in kind (from Council)	unknown	Yes.
ticket sales to event	40,000	No.

2

Please outline how your organisation intends to manage and be accountable for the funds allocated, should your submission be successful.

The Yellow Mountain Cross Country event has received in-kind support from Council for many years, including provision of a portable toilet block, putting road signs out and printing of maps for the event. This is the support we are seeking again for the 2024 event.
1- toilet block at Condobolin Auto Sports Club.
2- TMP & putting road sign out 3- Printing Maps.

PART D - Project Budget

Please provide a detailed budget for your project. It is important that you clearly identify expenses by type and that every effort is made to reasonably estimate the level of income expected from sources such as entrance fees and sponsorship.

Is project budget attached before? ☐ Yes ☒ No

Project Budget Summary:	Amount
Cash contributed by your organisation:	20,000
Cash from other sources: tickets.	$40,000
In kind contribution, approximate value e.g. Volunteer	$200,000
Amount requested from Lachlan Shire Council	in kind.
Total Cost of Project:	260,000

Authorisation:

I, JAMES Patton (print name)

certify that this application for funding was approved by the management committee of this organisation on

(insert Date).

Signed: [signature] Date: 12/06/24.

(3) Map- 200 Double sided A4 same as in 2023 - same maps
is Double sided A3 maps

July 2023 to June 2024

Community Donation & Event Support Policy - Authorisation register. Approved under delegated authority section 377 (1A) of the *Local Government Act 1993*				
Details	In-Kind Support $500 or less	Fee or Charge Concession $500 or less	Financial donation Less than $500 (12-month transition 1/8/2023 to 31/07/2024)	Notes
Central West Farming - Regional Women & Youth Conference		$ 360.00		50% Concession SRA Hall Hire
Koori Kids School Initiatives – NAIDOC week			$ 450.00	
Tottenham Central School			$ 100.00	
Lake Cargelligo Central School			$ 100.00	
Black Dog Ride Institute	$ 500.00			Donated by VIC
Total	**$ 500.00**	**$ 360.00**	**$ 650.00**	

LACHLAN SHIRE COUNCIL

FRAUD AND CORRUPTION CONTROL

POLICY

Table of Contents

1. BACKGROUND

The community expect public officials to perform their duties with honesty and in the best interests of the public. Corrupt conduct by a public official involves a breach of public trust that can lead to inequity, wasted resources or public money and reputational damage.

Lachlan Shire Council (Council) is committed to implementing and maintaining an integrity framework to prevent and eliminate fraud and corruption by internal or external parties in relation to council activities.

Message from the General Manager

The public, our fellow employees and other people we deal with are entitled to expect each of us to act with integrity and to protect resources, information, revenues, reputation and the public interest. Therefore, Council is committed to an honest and ethical environment that minimises fraud and corruption. Fraud and corruption are incompatible with our values and present a risk to the achievement of our objectives and the provision of our services to the public. Council has a zero-tolerance approach to fraud and corruption.

2. SCOPE

This policy applies to public officials of Council including councillors, staff, committee members, contractors, outsourced service providers, consultants, volunteers, and anyone performing work for Lachlan Shire Council.

3. OBJECTIVE

The Fraud and Corruption Control Policy 2024 aims to protect Council's revenue and assets, protect the integrity, security and reputation of Council and maintain a high level of services to the community by limiting Council's exposure to fraudulent or corrupt activities of any nature.

This policy complements the provisions of relevant Council policies including *Code of Conduct* policies for Staff and Councillors*, Conflict of Interest Policy*, *Gifts, Benefits and Bribes Policy, Public Interest Disclosure Policy, Procurement Policy*, Local Government Act and Regulations, guidelines and controls.

4. DEFINITIONS

Definitions for the purpose of this policy include the following:

Public Official: A public official is defined in Section 3 of the ICAC Act as an individual having public official functions or acting in a public official capacity.

Fraud Fraud is defined in *AS 8001-2008 and Corruption Control, 2008*, as "Dishonest activity causing actual or potential financial loss to any person or entity including theft of moneys or other property by employees or persons external to the entity where deception is used at the time, immediately

before or immediately following the activity. This also includes the deliberate falsification, concealment, destruction, or use of falsified documentation used or intended for use for a normal business purpose or the improper use of information or position for personal financial benefit".

Fraud can be defined as a deliberate and premeditated turn of events which involves the use of deception to gain advantage from a position of trust and authority. The type of events include: acts of omission, theft, the making of false statements, evasion, manipulation of information and numerous other acts of deception.

Corruption

Corruption is defined in *AS 8001-2008 Fraud and Corruption Control, 2008* as: "Dishonest activity in which a director, executive, manager, employee or contractor of an entity acts contrary to the interests of the entity and abuses his/her position of trust in order to achieve some personal gain or advantage for him or herself or for another person or entity. The concept of 'corruption' within this standard can also involve corrupt conduct by the entity, or a person purporting to act on behalf of and in the interests of the entity, in order to secure some form of improper advantage for the entity either directly or indirectly".

Corruption involves conduct that is dishonest, partial, a breach of public trust or the misuse of official information or material. To be corrupt, the conduct must also involve a criminal or disciplinary offence, provide reasonable grounds for dismissal or be a substantial breach of the Code of Conduct.

Corrupt Conduct:

Corrupt conduct, as defined in the *Independent Commission Against Corruption Act 1988* ("the ICAC Act"), is deliberate or intentional wrongdoing, not negligence or a mistake, involving or affecting a NSW public official or public sector organisation. While it can take many forms, corrupt conduct occurs when:

- a public official improperly uses, or tries to improperly use, the knowledge, power or resources of their position for personal gain or the advantage of others
- a public official dishonestly exercises his or her official functions, or improperly exercises his or her official functions in a partial manner, breaches public trust or misuses information or material acquired during the course of his or her official functions
- a member of the public influences, or tries to influence, a public official to use his or her position in a way that affects the probity of the public official's exercise of functions

- a member of the public engages in conduct that could involve one of the matters set out in section 8(2A) of the ICAC Act where such conduct impairs, or could impair, public confidence in public administration.

5. POLICY IN BRIEF

Council is committed to implementing a framework to prevent and eliminate fraud and corruption in relation to Council activities.

The key features of Council's Fraud and Corruption Management framework are made up of periodic risk assessments, periodic training, corruption prevention strategies, internal control systems, designated responsibilities and review arrangements

6. POLICY IN DETAIL

6.1 Approach

Council will adopt an agency-wide fraud and corruption control framework that is consistent with the NSW *Fraud and Corruption Control Policy*. In particular, Council is committed to:

- Implement internal controls that prevent, detect and respond to fraud and corruption, as part of its framework
- assess its fraud and corruption risks regularly, at least annually
- ensure all staff, including contractors, are aware of relevant fraud and corruption risks and are trained to understand Council's values, codes, policies and expectations of behaviour
- report annually to the Audit Risk and Improvement Committee (ARIC) on the status of the fraud and corruption control framework
- treat all complaints about, and instances of, fraud and corruption seriously. Council will cooperate with all relevant investigative and regulatory bodies and will take fair, proportionate disciplinary action against any employee or third party found to have engaged in fraud or corruption
- wherever practical, align to better practice advice issued by organisations such as the NSW Independent Commission Against Corruption, the NSW Ombudsman and Audit Office of NSW

6.2 Council Values and Business Practices

Council has a zero tolerance to matters of fraud and corruption. Matters proven to involve fraud or corruption will be dealt with in accordance with relevant legislative and policy requirements.

Council is committed to building and sustaining an ethical, efficient and effective culture where opportunities for fraud and corruption are minimised.

Council recognises that staff and Councillors understand what good conduct is and are committed to the highest standards of probity in management and operation of the Council. This plan aims to support Councillors and staff in achieving these standards.

Council has a comprehensive fraud and corruption management framework which aims to ensure public confidence and trust in the work of Council. Specifically, the fraud and corruption management framework:

- ensures that all Councillors, staff, contractors and suppliers to Council are aware of the standards of ethical behaviour required of them
- provides a mechanism for any party (internal or external to Council) to advise of potential ethical conflicts relating to Council's function
- provides systems to identify and manage risks within the organisation

6.3 Fraud and Corruption Review

Council operates in an environment of extensive contracting for goods and services, devolution of management control and authority, increased decision-making powers of many staff, and increasing access to confidential information through computer technology. It is essential that Council regularly identifies potential risks created by this environment, and ensures that the organisation's procedures, systems and controls are sufficient to counter any corruption risks identified.

The General Manager is responsible for initiating a review of Council's fraud and corruption risks, as detailed in Council's enterprise risk register, throughout business areas. This review is to be undertaken annually and will consider:

- internal controls and are they adequate
- the areas of council that may be most vulnerable to fraud and corruption and
- what may go wrong.

All staff, especially directors and section managers, are responsible for cooperating with the General Manager by identifying and treating fraud and corruption risks. It is not cost effective to endeavour to cover every possible risk of fraud and corruption. However, the risk assessment will identify priority areas for the allocation of resources to ensure that appropriate steps are taken to obviate foreseeable corruption risks.

6.4 Fraud and Corruption Risk Management Strategies

The General Manager is responsible for ensuring that appropriate fraud and corruption risk management strategies are in place and that resources are allocated as necessary to manage any risk of fraud and corruption identified.

6.5 Information and Training

Through an education and training program, Council aims to ensure that all staff have access to sufficient information to enable them to identify, prevent and report potential wrongdoing. The General Manager is responsible for ensuring that the education and training program is communicated throughout Council's operations.

The information, education and training program will include:

- Staff induction training
- Specialist and specific training for both high-risk functions and general training for all staff
- Information updates on policies, procedures and legislative requirements
- Policies that provide for efficient and thorough management of complaints and enquiries
- Inclusion of relevant information in Council's Annual Reports and website
- Inclusion of requirements in tendering documentation
- Ongoing reviews of contractor performance and adherence with Council policies and procedures

6.6 Detection

6.6.1 Auditing

Council has an Audit Risk and Improvement Committee and has appointed an internal auditor. The internal auditor is working through a program of audits based on an organisation wide risk assessment. Council has a Risk Management Policy in place that establishes the systems and processes required to manage the risks involved in Council's activities so as to maximise opportunities and minimise negative outcomes.

6.6.2 Reporting

Council's internal and external reporting system encourages a free flow of information through supervisory and management channels. Complaint handling includes frontline complaint handling, internal review and external review. Staff are made aware of available reporting procedures through training and induction processes. The reporting system includes the following tools:

- Complaints Management Policy
- Public Interest Disclosure Policy - designated public interest disclosures officers within Lachlan Shire Council are outlined in this Policy
- Code of Conduct policies for Staff and Councillors

7. ROLES AND RESPONSIBILITIES

7.1 The General Manager

The General Manager has overall responsibility for fraud and corruption control within Council. The General Manager shall be responsible to ensure:

- that appropriate fraud and corruption risk management strategies are in place;
- that resources are allocated as necessary to minimise any risk of fraud or corruption that may be identified;
- that ethical standards are set and communicated throughout the area of the Council's operations;
- reported fraud or corruption is investigated promptly, dealt with appropriately, and that policies or procedures are reviewed to prevent recurrence where necessary;

- all fraud and corruption risk management initiatives are implemented within the Council;
- that ICAC is notified of any matter suspected on reasonable grounds that concerns or may concern corrupt conduct. Under the Independent Commission Against Corruption Act 1988 the General Manager is under a duty to report to the ICAC any matter that the General Manager suspects on reasonable grounds, concerns or may concern corrupt conduct. Corrupt conduct is defined within the ICAC Act and includes fraud.

7.2 All Councillors, Staff, Contractors, Committee Members, Volunteers

Each individual has a responsibility to:

- adhere to ethical standards in their respective area and provide their colleagues with guidance and support as required;
- observe and support the requirements of the relevant Council policies and procedures;
- report all suspected fraud, corruption and inappropriate behaviour to a relevant Council Disclosure Officer under the *Public Interest and Disclosure Policy,* and/or the relevant Officer, which may be your Section Manager, Director, the General Manager, Mayor or an external agency such as the Office of Local Government, NSW Ombudsman or ICAC.

7.3 All Directors, Managers and Supervisors

All individuals with managerial or supervisory responsibilities, must ensure in their area of responsibility that:

- decisions or conduct are lawful;
- decisions or conduct are consistent with Council Policies/ Procedures and the Code of Conduct;
- all conflicts of interest are disclosed and managed so that outcomes are not affected by private gain; decisions or conduct can be justified in terms of the public interest; and
- decisions or conduct would withstand public scrutiny.

In addition to complying with all integrity-related policies including the Code of Conduct, employees are expected to cooperate with all initiatives aimed at preventing, detecting and responding to fraud and corruption. This includes risk assessments, training and education, audits and investigations and the design and implementation of controls.

Directors, Managers are supervisors are also expected to:

- ensure all agreed controls aimed at preventing, detecting and responding to fraud and corruption are in place
- alert the policy owner [or other suitable person] of any undocumented or emerging fraud and corruption risks
- ensure suppliers and contractors are aware of Council's policies and expectations in relation to fraud and corruption
- ensure all staff complete relevant training and are aware of fraud and corruption risks.

7.4 Audit Risk and Improvement Committee (ARIC)

The Audit Risk and Improvement Committee has responsibilities in accordance with its adopted Terms of Reference. ARIC is responsible for giving advice to the General Manager in relation to this policy and monitoring the fraud and corruption control framework.

8. FURTHER INFORMATION

Further information about this policy can be obtained by:

- contacting the Governance and Risk Officer
- contacting the Director Corporate and Community Services
- visiting the website of the NSW Independent Commission Against Corruption (ICAC) at www.icac.nsw.gov.au

9. RELATED DOCUMENTS

Related Council policies include:

- Code of Conduct policies, for Council Staff and for Councillors
- Complaints Management Policy
- Conflict of Interest Policy
- Gifts, Benefits and Bribes Policy
- Public Interest Disclosure Policy
- Procurement Policy
- Disposal of Assets Policy
- Local Preference Policy
- Risk Management Policy
- Privacy Management Plan
- Statement of Business Ethics

Related Legislation includes:

- Public Interest Disclosures Act 1994
- Local Government Act 1993
- Local Government (General) Regulation 2021
- Government Information (Public Access) Act 2009 (GIPA Act)
- Privacy & Personal Information Protection Act 1998 (PPIP Act)
- Independent Commission Against Corruption Act
- AS 8001-2008 Fraud and Corruption Control, 2008

Nothing in this policy limits any applicable legislation.

Greg Tory

GENERAL MANAGER

LACHLAN SHIRE COUNCIL

GIFTS, BENEFITS AND BRIBES POLICY

Name of Policy Further Information: ☎ 02 6895 1900 ✉ Email: council@lachlan.nsw.gov.au						Page 1 of 9
Version:	**Adopted:**	**Resolution:**	**Commencement Date:**	**Last Review Date:**	**Next Review Date:**	**Content Manager Ref:**
5	June 2024	YYYY/NNN	N/A	June 2024	June 2028	D24/NNNN

Table of Contents

1. BACKGROUND

Lachlan Shire Council (Council) is committed to providing a framework to prevent corruption in all its forms.

2. SCOPE

This policy applies to all Council public officials, including staff, councillors, committee members, contractors, volunteers, and anyone working and/or providing services on behalf of Council. Collectively they are referred to as council representatives.

The policy complements Council's related policies including Code of Conduct – Councillors, Code of Conduct- Staff, Conflict of Interest Policy, Fraud and Corruption Control Policy, Public Interest Disclosure Policy.

3. OBJECTIVE

This policy provides guidance in relation to gifts, benefits and possible bribes offered in the course of duty, and associated requirements and reporting.

4. DEFINITIONS

Public Official: A public official is defined in section 3 of the ICAC Act as an individual having public official functions or acting in a public official capacity. A Public Official of Council includes Councillors, staff, committee members, contractors, volunteers, and anyone working for or providing services on behalf of Council. Collectively they are referred to council representatives.

Gift or Benefit: A gift or benefit is anything of value. It may be considered any item, service, prize, hospitality or travel offered by a person or other entity that has an intrinsic value and/or a value to the recipient, a member of their family, relation, friend or associate. It includes gifts or benefits from, for example, contractors, customers, clients, applicants, suppliers, potential suppliers or external organisations.

Hospitality is the reception and entertainment of guests. It includes refreshments or a service provided or promised to be provided by an individual or organisation to another.

In considering the **value** of a gift, benefit or hospitality, it is the highest of:

- the cost to the giver
- the retail or replacement cost of the gift, benefit or hospitality
- the value of the gift or benefit to the recipient.

Council representatives should be mindful of the **cumulative value** of gifts, benefits and hospitality. For example, the cost of multiple coffees offered over the course of a year is likely to exceed the nominal value/monetary threshold for acceptance.

Bribe: A bribe, or bribery, is defined as receiving or offering any undue reward by, or to, any person in public office in order to influence his or her behaviour in that office, and to incline that person to act contrary to the known rules of honesty and integrity.

Nominal Value: Gifts and benefits of nominal or token value usually do not create a sense of obligation in the receiver that will influence, or appear to influence, the exercise of his or her official duties. Examples of gifts and benefits that could be regarded as having a nominal value include cheap marketing trinkets or corporate mementos that are not targeted specifically at the business of Council, such as inexpensive pens and pencils, notepads, calendars, keyrings, confectionary, modest hospitality such as tea or coffee (but not three course meals).

See Part 6 of Council's Code of Conduct policies for Councillors and Staff re "Gifts and Benefits of Token (nominal) Value".

5. POLICY IN BRIEF

Corruptly receiving a gift or benefit or bribe is an offence under both the common law and NSW legislation. The offence extends to the offering or seeking of a gift or benefit or bribe.

If public officials are offered a gift or benefit or bribe, where they believe the intention of the person was to bribe them or influence the way they work, they must report it immediately, to their Manager, Director, General Manager, or Mayor, in accordance with this policy and related Council policies and reporting procedures.

Under section 11 of the *Independent Commission Against Corruption Act 1988*, the General Manager must inform the ICAC about any matter that they suspect on reasonable grounds may concern corrupt conduct.

6. POLICY IN DETAIL

6.1 Nominal or Token Value

Council has set a nominal or token value for gifts and benefits in its Code of Conduct for Councillors, Delegates and Committee Members, and its Code of Conduct for Staff as follows:

- up to $50 (including GST) value for Council Employees or Volunteers (per individual in any 12 month period), in accordance with the Code of Conduct for Staff
- up to $100 (including GST) value for Councillors (per individual in any 12 month period), in accordance with the Code of Conduct for Councillors, Delegates and Committee Members.

Gifts or benefits considered as nominal or token value are exempted under this policy.

6.2 Refusing gifts, benefits and hospitality

Council representatives should not solicit or accept any gifts, benefits or hospitality that could be perceived as intended to influence them, or if they are more than token value. **Offers of money should never be accepted.**

Council representatives should always be mindful that people might want to cultivate a relationship with them because of their role. The best course of action is to politely refuse any gifts, benefits or hospitality, unless the conditions enabling acceptance can be met under this policy.

Gifts, benefits and hospitality that do not meet the exemption criteria of this policy or Code of Conduct should be refused, no matter how insistent the person making the offer. Such offers should also be declared and reported to management.

If gifts are provided in a way that is not possible for them to be returned, council representatives should make a declaration or other form of written record for their Director and General Manager, of the circumstances surrounding the receipt of the gift and how it was handled. After consultation with management, the gift might, for example, be donated to charity, disposed of, auctioned to staff or used as a raffle prize. It is preferable for a Manager, Director, General Manager, or other designated officer, to make the determination, which should be documented.

6.3 Risk Factors

There are a number of general risks associated with gifts and benefits, including hospitality, such as:

- the risk and/or perception that council representatives might be unduly influenced or open to bribery
- peoples' tendency to feel a sense of indebtedness and reciprocate when they are given something, even where the gift, benefit, hospitality is of a modest value
- the conflict of interest that could be created between a council representatives duty and their personal interests because of the relationship with the gift-giver that could form
- the possibility of benefitting some individuals or organisations through influenced or unjust decisions, while unfairly disadvantaging others
- the risk a council representative is compromised once they have accepted a gift (for example, they could be subject to threats of exposure unless they continue to provide preferable treatment to the giver)
- the potential for an organisation's independence and reputation to be brought into disrepute.

There are also specific risks that relate to a council representative's work. Roles that have broad discretionary powers, and/or involve functions such as regulation, procurement, contract management and revenue collection, have high levels of risk attached to them. Council representatives working in high-risk areas should decline any offers of gifts, benefits or hospitality, even when they have a low value.

Relevant third parties, such as contractors and subcontractors, must be informed that the offering and/or acceptance of gifts, benefits and hospitality will not be permitted, and that any attempts by council representatives to facilitate such contributions must be reported.

6.4 General Rules

Council's general advice to representatives is that gifts or benefits of any kind should be declined in accordance with this policy and Council's Code of Conduct policies. You must:

- Always report an offer of gifts, benefits or possible bribe
- Not seek or accept a bribe;
- Not seek gifts or benefits of any kind;
- Not accept an offer of money, regardless of the amount;
- Not accept any gift or benefit that may create a sense of obligation on your part, or may be, or perceived to be, intended or likely to influence you in carrying out your public duty.

The recipient is responsible for reporting gifts or benefits offered or received, for inclusion in Council's Gifts and Benefits Register and for determination of any further action applicable.

Council has a form to report Gifts and Benefits which must be submitted to the General Manager.

Council's Gifts and Benefits Register is maintained by the Executive Assistant to the General Manager and the Mayor.

6.5 Gifts and Benefits – Exemptions under this policy

A reference to a gift or benefit under this policy does not include the following, in accordance with Part 6 of the Council's Code of Conduct policies for Councillors and Staff:

a) items with a value of $50 (including GST) or less for staff (per individual in any 12 month period), or $100 (including GST) or less for councillors (per individual in any 12 month period), are considered nominal/token value and exempt under this policy;

b) a political donation for the purposes of, and in accordance with, the Electoral Funding Act 2018 (for Councillors);

c) a gift provided to the council as part of a cultural exchange or sister-city relationship that is not converted for the personal use or enjoyment of any individual council official or someone personally associated with them;

d) a benefit or facility provided by the council to an employee or councillor;

e) attendance by a council official at a work-related event or function for the purposes of performing their official duties,

f) free or subsidised meals, beverages or refreshments provided to council officials in conjunction with the performance of their official duties such as (but not limited to):

- the discussion of official business
- work-related events such as council-sponsored or community events, training, education sessions or workshops
- conferences

- council functions or events
- social functions organised by, for example, council committees or community organisations.

7. REPORTING OF AN OFFERING

In accordance with this policy, and related Council policies including *Code of Conduct, Fraud and Corruption Control Policy* and *Public Interest Disclosure Policy*, you must report any offering in the course of duty - of any gift, benefit or possible bribe.

7.1 Reporting of Offering of Gifts or Benefits

If a representative of Council including Councillor, staff, contractor, committee member or volunteer is offered a gift or benefit that is more than of nominal value, the following procedure must be followed:

a) Refuse the gift or benefit;

b) Make notes immediately after the approach has been made setting out as clearly as possible what occurred, including:

- Date, time and place of the offer;
- To whom the offer was made;
- The name and details of the person who offered the gift or benefit;
- The estimated monetary value of the gift or benefit;
- The response to the offer;
- Any other relevant details of the offer, and;
- Sign and date the notes, keeping a copy for your own records.

c) Inform the Mayor, or General Manager, or the relevant Director (in the case of employees, contractors and volunteers), providing a copy of your signed notes.

d) The General Manager must ultimately be informed of any offer(s). If the matter relates to the General Manager, then it should be referred to the Mayor.

7.2 Reporting of Offering of Possible Bribes

If a representative of Council, including a Councillor, staff, contractor, committee member or volunteer believes that they have been offered a possible bribe, the following procedure must be followed:

a) Refuse the possible bribe

b) Make notes immediately after the approach has been made setting out as clearly as possible what occurred, including:

- Date, time and place of the offer
- To whom the offer was made

- The name and details of the person who offered the possible bribe
- The response to the offer
- Any other relevant details of the offer, and
- Sign and date the notes, keeping a copy for your own records.

c) Inform the General Manager and your relevant Director, and provide a copy of your signed notes. If the matter relates to the General Manager then it should be referred to the Mayor.

d) The General Manager (or Mayor, if the matter relates to the General Manager) must be informed of the offer, and subsequently must inform the following as may be required:

- The Independent Commission Against Corruption (ICAC);
- NSW Police.

Complaints regarding bribery should be referred to the General Manager. Should the complaint concern the General Manager, then it should be referred to the Mayor.

Once the matter has been reported and it is apparent that an extended investigation is not likely, the following will occur:

- Council will make the person who offered the possible bribe aware that bribery is a serious offence and that such behaviour will not be tolerated by Council;
- if any further contact with the person who offered the possible bribe is required, a supervisor or colleague will accompany the employee who was subject of the offer;
- if any threats are made towards the employee concerned, every effort will be made to ensure their safety, including informing the NSW Police and the ICAC.

8. FURTHER INFORMATION

Further information about this policy can be obtained by:

- contacting the Director Corporate and Community Services or the General Manager
- contacting the Governance and Risk Officer
- contacting ICAC, email icac@icac.nsw.gov.au, or website: https/icac.nsw.gov.au

9. RELATED DOCUMENTS AND LEGISLATION

Related Council policies include:

- Code of Conduct for Council Staff
- Code of Conduct for Councillors
- Fraud and Corruption Control Policy
- Conflict of Interest Policy
- Public Interest Disclosure Policy

Related Legislation includes:

- Public Interest Disclosure Act 2022
- Local Government Act 1993
- Local Government (General) Regulation 2021
- Crimes Act
- The *NSW Government Supplier Code of Conduct* makes explicit that suppliers must not at any time offer or provide any financial or non-financial benefits to NSW public officials.

10. RIGHT TO VARY/TERMINATE

Council reserves the right to vary or terminate this policy at any time.

Nothing in this policy limits any applicable legislation.

Greg Tory

GENERAL MANAGER

LACHLAN SHIRE COUNCIL

PROCUREMENT POLICY 2024

Table of Contents

1. BACKGROUND

The purpose of this policy is to provide the principles under which Lachlan Shire Council (Council) makes its procurement decisions and conducts its procurement activities.

2. SCOPE

This policy applies to all Staff, Councillors, Consultants, Contractors, and anyone involved in Council procurement activities at any level.

This policy applies to all of Council's procurement activities as they relate to the acquisition and use of goods and services, including (but not limited to):

- Tendering;
- Contracts and payments;
- Quotations;
- Goods or services procured by third parties, such as contractors, acting as representatives of Council;
- Expressions of Interest for goods or services;
- Council credit cards;
- Fuel cards;
- Charging purchases to an account that Council may hold with a supplier;
- Purchase orders;
- Petty Cash

3. OBJECTIVE

The objectives of the Procurement Policy are to:

- Ensure the procurement process is auditable. The process is open, fair, transparent, consistent, and in accordance with Council's Code of Conduct and all relevant Council policies and procedures;
- Comply with the Local Government Act 1993 (NSW), Local Government (General) Regulation 2021 (NSW), and other relevant legislative requirements;
- Comply with the requirements of the *Modern Slavery Act 2018* (NSW) and the *Guidance on Reasonable Steps* issued by the Anti-Slavery Commissioner, including associated reporting, model tender clauses and model contract clauses;
- Ensure competitive procurement of goods, works and services to maximise community benefit;
- Ensure value for money is delivered. Funds are spent effectively and economically, taking into account price and non-price factors (such as after sales service, warranty, safety, repair costs, spare parts, environmentally sustainable);
- Ensure appropriate risk management, including segregation of duties in the requisitioning, approval and payment functions.

4. DEFINITIONS

Contract:	The written agreement between the Council (as the purchaser) and the service / goods provider.
Expression of Interest:	The process of seeking non-binding information from proponents capable of providing specified goods/services which may include indicative pricing.
Modern Slavery:	As defined under the *Modern Slavery Act 2018* including obligations of Council under the Act
Procurement:	The acquisition of works, goods and services. Includes the evaluation of suppliers, preparation of purchase orders, receipt of goods / services and approval of payment.
Purchase Order:	The authority to the supplier to supply and invoice items at the prices agreed via the quotation process. The purchase order is a legal and binding contractual agreement on all parties.
Quotation:	A formal statement submitted by the proponent setting out a fixed cost or schedule of rates for the specified procurement of goods and/or services.
Tender:	Written submissions for procurement valued at $250,000 and over, invited and administered in accordance with the Local Government Act 1993 and associated Regulations.
Tender Panel:	A panel comprising a minimum of three (3) appropriately experienced and responsible officers with the expertise to assess and recommend the acceptance or rejection of tenders valued at $250,000 and over

5. POLICY STATEMENT

Council is committed to procurement practices that achieve the best possible value for money, and employ highly transparent, accountable and ethically sound processes. Council will conduct evaluations of the whole-of-life cost of purchases, and ensure that best practice procurement processes are communicated, understood and adhered to by all parties.

Council will procure goods and services in a financially, environmentally and socially sustainable and acceptable manner.

Council will discontinue all dealings with suppliers it reasonably suspects of having engaged in unethical conduct.

Where appropriate Council will also take further action against these suppliers, including legal action and, reporting suspected fraud or corruption to the Police and the Independent Commission against Corruption.

6. POLICY IN DETAIL

6.1 Responsible financial management

The principle of responsible financial management is to be applied to all procurement activities. Council funds are to be used efficiently and effectively to procure goods, services and works and every attempt must be made to contain the cost of the procurement process without compromising any of the procurement principles set out in this policy.

6.2 Procurement activities – Authorisations

All procurement activities by employees of Council, require prior authorisation by officers with approved financial delegations, only up to their delegated amount, and where the procurement is provided for in Council's budget

The General Manager may incur financial expenditure on behalf of Council within authorised delegations, where expenditure has been provided for in Council's approved budget, or genuine emergency or hardship provisions.

All delegations are to be recorded in a Register of Delegation of Authority.

6.3 Value for Money

Procurement activities are to be carried out on the basis of delivering value for money. This means minimising the total cost of ownership over the lifetime of the good or service consistent with acceptable quality, reliability, safety and delivery considerations.

Contracts will be sized and packaged with a view to maximising the economies available through the quotation/tender process and ensuring a competitive process.

Council is committed to ensuring funds are spent effectively and economically by taking into account price and non-price factors. Non-price factors may include (but are not limited to):

- Quality
- Reliability and reputation of supplier
- Availability and delivery time
- After sales service
- Warranty
- Safety
- Trading terms and discounts
- Whole of life cost of the goods and services
- Sustainability principles

6.4 Ethical, Environmental and Sustainable

Procurement decisions should incorporate principles of ethical, environmental, and sustainable sourcing, where feasible, including:

- The use of locally sourced services and products where practical
- Eliminating modern slavery in the supply chain
- Reuse, renewable or recoverable resources
- Minimising packaging

- Minimising harm to the environment
- Minimising waste

6.5 Modern Slavery

In accordance with the *Modern Slavery Act 2018*, and the *Guidance on Reasonable Steps* issued by the Anti-Slavery Commissioner, Council will

- Take reasonable steps to ensure that the goods and services procured are not the product of modern slavery
- Provide information as required in its Annual Report
- Include model GRS clauses in its tendering and contract management activities

6.6 Conflict of Interest and Business Ethics

All procurement activities must manage any real, potential or perceived conflict of interest under this policy in accordance with Council's related policies including Code of Conduct, Conflict of Interest Policy, Statement of Business Ethics Policy, Gifts Benefits and Bribes Policy, Fraud and Corruption Control Policy, Public Interest Disclosure Policy, and legislative requirements.

6.7 Procurement Requirements

Where the total cost of a contract over the life of the contract is likely to exceed $250,000 inclusive of GST, a tender is required.

In emergency situations, the General Manager has the discretion to vary the process in writing where required (up to $250,000).

All purchases may be subject to Council's "Local Preference Purchasing Policy".

Table 1 – Procurement Requirements (All amounts are inclusive of GST)

Invoice or order splitting to avoid quoting or tendering requirements is not permitted under Legislation

Purchase Value	Process	Quotation Type
$0 - $500	Work Order & staff member's full name to be provided to supplier and noted on invoice. Purchase Orders are encouraged but not necessary.	Not needed
$501 - $4,999	Purchase Order	One (1) written or verbal quote. Verbal quote requires a legible diary
$5,000 - $49,999	Purchase Order	Invite two (2) written quotes
$50,000 - $249,999 (Refer also ** **Note 2**)	Purchase Order – attach 3 x Formal Quotes with specification	Invite three (3) written quotes. Formal tender for works/services provided by Council staff $150,000 and above(**Note 2 below)
$250,000 and above (Refer also ***Note 1** and ** **Note 2**)	Prescribed agency purchase or Tender in accordance *Local Government Act 1993 (NSW)* and Part 7 *Local Government (General) Regulations 2021*	Formal Tender Process (unless approved exemption) Prescribed agency purchase or Tender in accordance *Local Government Act 1993(NSW)* and Part 7 *Local Government (General) Regulations 2021*

*** Note 1:** Contracts entered into for the purpose of responding to /recovering from a declared natural disaster within 12 months of the declaration have a tender threshold of $500,000 including. GST. Refer to Office of Local Government Circular 20-03 Amendments to the *Local Government (General) Regulation 2021* to increase the tendering exemption threshold for contracts for bushfire recovery and operations, dated 24 January 2020.

****Note 2:** Request for Tender is required for contracts $150,000 and above involving the provision of Services where those Services are, at the time of entering the contract, performed by Council officials.

Quotes are not required if you engage one of the suppliers who are on the Local Government Procurement (LGP) contract panel BUT you must:

- Issue a correctly authorised Purchase Order
- quote the LGP contract number on the Purchase Order

Quotes are not required when there is genuinely one supplier but you must:

- Issue a correctly authorised Purchase Order
- quote the "sole supplier" on the Purchase Order

6.8 Quotations

The assessment of quotations will be objective, consistent, documented, transparent and undertaken in accordance with Council's Procurement Procedures.

Council will only accept one conforming quotation from each supplier. Suppliers will not be given an opportunity to re-quote for the supply of goods and services unless the scope of work changes.

Quotations for alternate options may be accepted for consideration, only if a conforming quotation has been provided. Council will not be bound to accept or consider alternate quotations. If a conforming quotation is not accepted, to ensure an equitable and transparent process Council may decide to readvertise for quotations incorporating alternate option(s), if it is considered that more than one supplier is available.

6.9 Tendering

All Tenders will be conducted in accordance with Section 55 of the *Local Government Act 1993 (NSW),* Local Government (General) Regulation 2021 (NSW), the NSW Office of Local Government Tendering Guidelines, and the Modern Slavery Act 2018 requirements.

Whilst a formal tendering process is not required for purchases under $250,000, a formal tendering process can be utilised for any purchase under the threshold. This is advisable in the following situations:

- The purchasing amount is close to $250,000
- The purchasing amount is likely to exceed $250,000 over the life of the contract.
- The goods or services are of significant public interest
- The purchase may be considered to be controversial or contentious
- The procurement process is complex
- The expected price of procurement is unknown
- Contracts $150,000 and above involving the provision of Services where those Services are, at the time of entering the contract, performed by Council officials

6.10 Prescribed Agencies

Section 55 of the *Local Government Act 1993* (NSW) provides Councils with an exemption from tendering requirements where such items are available under contract by prescribed authorities. Prescribed agencies include Local Government Procurement, Regional Procurement, and Procurement Australia Pty Ltd.

Prescribed agencies seek to undertake group tenders on behalf of NSW Councils to obtain competitive contracts from time to time. Council may utilise these supply arrangements where appropriate.

When using Prescribed Agencies the agency contract number is to be quoted on the purchase order so that the supplier is aware that the procurement is under this arrangement.

6.11 Exemptions

Exemptions from following Procurement requirements under this policy include the following:

- **To assist Council in Natural Disaster Response.** Section 170A of the *Local Government (General) Regulation 2021* provides Council with an exemption from tendering requirements for a contract of up to $500,000, if the contract is primarily for the purpose of response to or recovery from a declared natural disaster, and is entered into within 12 months after the date on which the natural disaster is declared.
- Ongoing invoices for contracted periods e.g. electricity and telephone accounts, insurance premium and excess payments, rent payments;
- Subscription and memberships – although review of the necessity of these items must occur prior to renewal;
- Legal advice and services
- Reimbursements for approved expenditures

- Other exemptions permitted under Section 55 of the *Local Government Act 1993* (NSW)

7. FURTHER INFORMATION

Further information about this policy can be obtained by:

- Contacting the Governance and Risk Officer
- Contacting the Director Corporate and Community Services
- Contacting the Office of Local Government
- Contacting the NSW Independent Commission Against Corruption (ICAC)

8. RELATED DOCUMENTS

Related Council policies include:

- *Code of Conduct for Council Staff*
- *Code of Conduct for Councillors*
- *Conflict of Interest Policy*
- *Gifts, Benefits and Bribes Policy*
- *Fraud and Corruption Policy*
- *Credit Card Policy*
- *Disposal of Assets Policy*
- *Local Preference Policy*
- *Statement of Business Ethics Policy*
- *Public Interest Disclosures Policy*
- *Terms and Conditions of Business*

Related Legislation includes:

- *Local Government Act 1993* (NSW)
- *Local Government (General) Regulation 2021* (NSW)
- *Modern Slavery Act 2018* (NSW)
- *Guidance on Reasonable Steps* issued by the Anti-Slavery Commissioner
- *Government Information (Public Access) Act 2009* (NSW)
- *Competition and Consumer Act 2010*
- *Tendering Guidelines for NSW Local Government* 2009, issued by Department of Premier and Cabinet (Local Government).

9. RIGHT TO VARY OR TERMINATE

Council reserves the right to vary or terminate this policy at any time.

Nothing in this policy limits any applicable legislation.

Greg Tory

GENERAL MANAGER

LACHLAN SHIRE COUNCIL

DISPOSAL OF ASSETS POLICY

Table of Contents

1. BACKGROUND

Lachlan Shire Council (Council) is committed to ensuring a systematic and auditable process for the disposal of Council assets when no longer required.

2. SCOPE

This policy applies to all staff, councillors, contractors, and anyone who is involved in the disposal of surplus Council assets.

This policy does not apply to land or real property. Disposal of land or buildings is to be conducted in accordance with legislative requirements and resolution by council.

3. OBJECTIVE

The objective of this policy is to ensure that Council's disposal of surplus assets activities are conducted with probity and transparency, comply with legislative requirements, and ensure optimal value to the Lachlan Shire community.

4. DEFINITIONS

Asset: **For this policy** an asset is defined as any item or resource owned and/or controlled by council (excluding land or real property). Assets referred to in this policy encompass all items of value to Council. This includes, but is not limited to, plant and equipment, office equipment, office furniture and stock items.

5. POLICY IN BRIEF

This policy provides guidance for the disposal of surplus Council assets, and recognises that:

- High standards of ethical practice and behaviour are essential in disposing of Council assets
- Disposal practices should be undertaken in accordance with legislative requirements, and in a manner that is clear and documented
- Asset disposal practices should aim to optimise the value to the broader Lachlan Shire community.

6. POLICY IN DETAIL

6.1 General Guidelines

All asset information should be reviewed prior to disposal to ensure informed decision making.

Items of historical or cultural significance should be carefully considered, and in accordance with relevant guidelines and regulations.

Any dangerous or hazardous goods are to be disposed in accordance with manufacturers' recommendation and legislative requirements. Expert advice should be obtained from Council's waste or environment officers as needed.

Ensure that all prospective purchasers are aware that the sale of assets is on the basis of "as is" and at the purchaser's risk. Purchasers are to rely on their own enquiries regarding the condition and workability of assets. No warranty or after sales service is to be offered on the disposal of any assets.

6.2 Identifying Surplus Assets

Council will regularly review the assets it holds to ensure they are fit for purpose. An asset can be deemed surplus to requirements for varying reasons, including:

- It has reached thresholds for Council's Plant and Equipment or vehicle replacement
- It has no identifiable future use, past its expiry, obsolete or inefficient
- It is unserviceable or uneconomical to repair
- It does not meet current work health and safety requirements
- It no longer complies with relevant environmental or quality standards

6.3 Review of Alternative Use

Prior to disposing of an asset, reasonable efforts will be taken to ensure that no other area of Council operation requires the asset.

6.4 Donation to charities and community organisations

Donations may be considered after exploring all avenues for recouping fair value to Council.

Low value surplus assets, with a cumulative value of up to $5,000, may be donated to charities and community organisations.

To ensure due process, charities and community organisations will be invited to submit a proposal for the items, with all groups treated equitably. Once determined the donation requires authorisation by the General Manager.

6.5 Preparing Assets for Disposal

- Prior to disposal, assets must be thoroughly checked to ensure they do not contain the following:
- Additional items not intended for sale
- Confidential documents or any other Council documents
- Council software, files or data (which may lead to a breach of licence, or contain confidential data or Council information)
- Hazardous material
- All Council branding or identifying marks should be removed where feasible.

6.6 Stock Items and Spare Parts

- Store personnel should be notified if disposal of an asset impacts stock items.
- Spare parts held for a particular asset should be disposed in conjunction with the asset.

6.7 Methods of Disposal

Disposal of assets should be conducted in a manner that maximises returns and ensures transparent and effective competition. Methods of disposal include (but are not limited to):

- Public Auction: assets with cumulative estimated value up to $249,999, or as determined by council.
- Tender: Assets valued at $250,000 or more must be disposed by tender in accordance with legislative requirements. Assets with estimated cumulative value under $250,000 may also be disposed by tender.
- Donation: – assets valued up to $5,000, by invitation to submit proposal, to charity or local community organisations
- Re-purpose: assets valued up to $5,000 may be re-purposed within Council or associated committee or user group, by inviting a documented proposal for the Committee/user group.
- Trade-In or as determined by council, assets including motor vehicle, plant and equipment
- Negotiated sales: assets valued up to $5,000 may invite proposals from interested parties including Rural Fire Service or other councils
- Landfill or destruction: assets of no economic value or deemed unsafe

The General Manager has the delegated authority to approve the disposal of assets and the appropriate method of disposal, as shown in Table 1. The General Manager may sub-delegate this authority where deemed appropriate.

The method of disposal will be selected to maximise the public benefits of disposal, considering social, economic and circular economy principles to minimise environmental impact. Where the cost of disposal outweighs the potential financial return to Council, efforts will still be made to re-use items, as outlined in Table 1 under $5,000 in value. Disposal to landfill should be a method of last resort, unless the item presents a risk to health and safety.

To ensure the process of disposal is at all times open and transparent, the decision and reasons for selecting a particular method of disposal will be documented and records saved, along with a register of all disposed assets.

The assessment of proposals, quotations and tenders must be documented and objective, consistent, and transparent. Council will only accept one quotation from potential purchasers, and potential purchasers will not be given an opportunity to re-quote.

Where items are to be disposed of via auction, a reserve price will be set by **the General Manager or their authorised delegate**, considering the advice of the auctioneer.

No warranty is to be provided on assets being disposed.

Table 1 – Disposal methods

Estimated Asset Value, (incl. GST)	Methods	Required Standard
Up to $5,000	Re-purpose of asset within Council or associated committee or user group	Invite documented proposal from Committees/user groups
	Donation of asset to charity or community organisation	Invite documented proposal from charities/community organisations
	Expression of Interest /Acceptance of quotes	Promoted via Council's website and social media. Invite proposals (including from, for example, Rural Fire Service, other councils). Written quotation required from potential purchaser(s)
	In-house tender	Promoted and executed via internal means. Items to be collected at no expense to Council.
	Public sale /giveaway	Promoted via Council's website and social media. Items to be collected at no cost to Council.
Up to $249,999	Public Auction	Conducted via registered auctioneer or registered online auction site
	Public Tender, in accordance with legislative requirements	Conducted via appropriate public advertising which may include Tender Link and subject to acceptance by Council
$250,000 or more	Must be by Public Tender, in accordance with legislative requirements	Conducted via appropriate public advertising which may include Tender

Estimated Asset Value, (incl. GST)	Methods	Required Standard
		Link and subject to acceptance by Council

(Note: This policy does not apply to land or real property. Disposal of land or buildings is to be conducted in accordance with legislative requirements and resolution by Council)

6.8 Staff, Contractors and Councillors

Disposal of assets to staff, contractors, committee members, councillors, or their relatives, partners, families, friends or associates, should not occur outside of a public process.

The Independent Commission against Corruption (ICAC) recommends that invitations to bid for the purchase of any surplus Council assets should not be limited to staff, contractors or to elected officials. Members of the public must also be provided with the opportunity to compete for the purchase.

6.9 Conflicts of Interest

A conflict of interest exists where a reasonable and informed person would perceive that a member of Council staff or an individual councillor could be influenced by a private interest when carrying out their public duty. Members of Council staff or individual councillors involved in the procurement process must avoid any conflict of interest.

Any conflict of interest, whether real, perceived, potential, pecuniary or non-pecuniary, involving a member of Council staff or an individual councillor, their spouse, relative, partner, friend or business associate, must be declared and must be dealt with in accordance with Council's policies including Code of Conduct, Conflict of Interest Policy.

7. FURTHER INFORMATION

Further information about this policy can be obtained by:

- contacting the Governance and Risk Officer
- contacting the Director Corporate and Community Services

8. RELATED DOCUMENTS

Related LSC policies include:

- *Code of Conducts for Councillors and Staff*
- *Procurement Policy*
- *Local Preference Policy*

- *Gifts, Benefits and Bribes Policy*
- *Fraud and Corruption Control Policy*
- *Conflict of Interest Policy*
- *Public Interest Disclosure Policy*
- *Modern Slavery Policy*
- *Statement of Business Ethics*

Related Legislation includes:

- *Local Government Act 1993 (NSW)*
- *Local Government (General) Regulation 2021 (NSW)*
- *Government Information (Public Access) Act 2009 (GIPA Act)*
- *Tendering Guidelines for NSW Local Government* issued by Department of Premier and Cabinet (Local Government)
- *Modern Slavery Act 2018 (NSW)*

9. RIGHT TO VARY OR TERMINATE

Council reserves the right to vary or terminate this policy at any time.

Nothing in this policy limits any applicable legislation.

Greg Tory

GENERAL MANAGER

LACHLAN SHIRE COUNCIL

LOCAL PREFERENCE PURCHASING POLICY

Table of Contents

1. BACKGROUND

As a public authority Lachlan Shire Council (Council) is required to comply with legislative requirements in the procurement of goods and services, including the Local Government Act 1993 (NSW), Local Government (General) Regulations 2021 (NSW), and the Competition and Consumer Act 2010.

Council seeks to support local suppliers and contractors through Council's procurement practices. This policy outlines how that support may be provided in the procurement assessment process.

2. SCOPE

This policy applies to all staff, contractors, consultants, councillors, and anyone involved in Council procurement activities.

3. OBJECTIVE

This policy outlines a range of criteria and weightings that can be applied in an assessment process of tenders and quotations called in compliance with legislative requirements. This policy recognises that it is important that Council staff, consultants, contractors, councillors, and anyone involved in Council procurement, fairly and equitably set and apply that criteria.

4. DEFINITIONS

Criteria: An attribute/characteristic that is comparable across a range of suppliers for a particular good or service. As a general rule a minimum of three criteria will be applied to assist in comparing suppliers.

Local Supplier: A supplier is defined as local when they have an office located within the Lachlan Shire local government area.

Quotation: A fixed price or schedule of rates provided by a supplier for the supply of goods or services, for procurements up to a cumulative total value of $249,999 (including GST).

Tender: A public competitive process for the supply of goods or services, conducted in accordance with legislative requirements, and must be used for procurements with cumulative value of $250,000 (including GST) or more. The tender process may be used for any procurements as preferred.

Weightings The percentage weighting given to each criterion in the assessment process.

5. POLICY IN BRIEF

Council is committed to providing best value services to the community. Best value does not always mean lowest price as there are many other factors that can be considered in selecting a provider of goods or services.

These factors include items such as relevant experience, financial resources, local knowledge, impact on the local economy and legislative responsibilities. These factors are all assessment criteria that may be used in the evaluation of quotations and tenders for goods and services to Council.

Council policy intention is to source goods and services preferably from suppliers and contractors within the Lachlan Shire, secondly from adjoining local government areas (LGAs) due to the high level of interdependence between the LGAs, and thirdly from outside the region.

Due to legislation such as the Competition and Consumer Act 2010, the purpose of which is to enhance the welfare of Australians through the promotion of competition and fair trading and provides for consumer protection, it is important that Council supports local suppliers where Council is of the opinion that it can support such a selection. This support will be demonstrated by the application of selection criteria to the assessment of the procurement decision.

The responsibility for the selection of the criteria and associated weightings for a quotation or tender assessment will rest with Council staff overseeing and evaluating the procurement process, subject to any matters reported to the elected Council for determination.

6. POLICY IN DETAIL

6.1 Local Supplier- Consideration

This policy supports local suppliers, where it is considered the benefits of that support to the Lachlan Shire community outweigh any additional costs incurred in the procurement of the goods and services.

Council will include in its procurement process (including formal quotations and tenders), an evaluation criterion for “Social and Community” that identifies attributes that reflect the supplier’s presence and economic contribution to the Lachlan Shire. The criteria applied to procurement decisions will include recognition of the impact of the procurement decision on the local economy through evaluating the benefit of that procurement to the local economy.

The criteria for a procurement decision may include, for example, the following “Social and Community” attributes:

- *Knowledge and experience with the local conditions, whether the supplier is a locally based business and/or whether they have worked locally*
- *Social impact on the local economy, for example local jobs created and a local office*
- *Level of local and Australian content, whether products and materials are sourced locally*
- *Alignment with Council’s Community and Strategic Plan (CSP)*

A weighting of 10% will be applied to local suppliers under the "Social and Community" criterion in any purchasing decision (including quotation and tender assessment), where there is considered to be the potential for a significant impact on the local economy through a Council procurement decision.

In assessing overall value for money in any procurement, the following non-price considerations should be also be taken into account (where relevant):

- Availability and access to after-sales service and maintenance
- Quality, type and availability of goods or services
- Advantages in dealing with a local supplier, including administrative and operational efficiency
- the proportion of local content to be supplied
- whole-of-life costs of the purchase or contract
- compliance with specifications, guidelines and requirements
- the supplier's knowledge, experience and ability to fulfil the requirements of the contract or purchase
- the supplier's commitment to supporting local businesses and the local economy through subcontracting and other supplier arrangements
- net benefits to the Lachlan Shire, including economic benefits

6.2 Prescribed Procurement Contracts

A number of supply and service contracts are available through tenders completed by the NSW State Government, the Central West Joint Organisation, and Local Government Procurement (LGP), with LGP being a fully owned subsidiary of Local Government NSW.

Council supports the use of prescribed contracts due to the reduction in tendering timeframes and cost benefits typically achieved through bulk purchasing.

Where purchases are conducted through these contracts Council accepts that the social and community criterion may not be able to be assessed as the evaluation has already been completed by the State Government or LGP - however if possible and relevant, a 10% local supplier discount preference could be applied.

6.3 Environment, Social and Economic Impacts

In addition to consideration of the impact on the local economy any Council procurement decision will also provide consideration to the environmental, social and economic impacts of that decision.

7. FURTHER INFORMATION

Further information about this policy can be obtained by:

- contacting the Governance and Risk Officer
- contacting the Director Corporate and Community Services
- contacting the General Manager

8. RELATED DOCUMENTS

Related LSC policies include:

- *Codes of Conduct policies –Councillors and Staff*
- *Conflict of Interest Policy*
- *Gifts, Benefits and Bribes Policy*
- *Fraud and Corruption Control Policy*
- *Procurement Policy*
- *Disposal of Assets Policy*
- *Modern Slavery Policy*
- *Statement of Business Ethics*
- *Terms and Condition of Business*

Related Legislation includes:

- *Local Government Act 1993*
- *Local Government (General) Regulation 2005*
- *Tendering Guidelines for NSW Local Government 2009*
- *Competition and Consumer Act 2010*
- *Modern Slavery Act 2018*
- *Guidelines on Reasonable Steps issued by the Anti- Slavery Commissioner.*

9. RIGHT TO VARY/TERMINATE

Council reserves the right to vary or terminate this policy at any time.

Nothing in this policy limits any applicable legislation.

Greg Tory

GENERAL MANAGER

LACHLAN SHIRE COUNCIL
Wiradjuri Country

LACHLAN SHIRE COUNCIL
DATA BREACH POLICY

Table of Contents

1. POLICY OBJECTIVES

1.1 The objective of this policy is to:

1.1.1. Outline how Lachlan Shire Council (Council) will identify, assess, manage, and respond to data breaches, particularly those involving personal information in accordance with the requirements of the Privacy and Personal Information Protection Act 1998 (PPIP Act).

1.1.2. Provide detail about:

a. what constitutes an eligible data breach under the PPIP Act;

b. the roles and responsibilities within Council for reporting, reviewing and managing data breaches; and

c. the steps involved in responding to a data breach and reviewing systems, policies and procedures to prevent future data breaches.

1.1.3. Ensure Council's compliance with the PPIP Act, the Health Records and Information Privacy Act 2002 (HRIP Act) and the Privacy Act 1988 (Cth) (Privacy Act) as governed by the Office of the Australian Information Commissioner (OAIC) and NSW Information and Privacy Commission (IPC), regarding handling personal and health information.

2. SCOPE

This policy applies to all staff and contractors of Council, including Councillors, volunteers, contractors and third party providers who hold personal and health information on behalf of Council.

2.2 This policy includes Council data held in any format (paper based or electronic) however, it does not apply to information that has been classified as public.

2.3 Depending on the type and extent of the data breach, management of public relations may be required, including coordinating the timing, content and method of public announcements and similar activities. These activities are outside the scope of this Policy, which is limited to the immediate internal responses of business units.

3. POLICY STATEMENT

3.1 Council is committed to ensuring, as far as practicable, that the data it holds is secure from potential data breaches and will regularly review, develop, maintain and test its systems and procedures to support data security and this Policy.

3.2 Having a data breach response policy is part of establishing robust and effective privacy and information governance procedures. Effective breach management assists Council in avoiding or reducing possible harm to both the affected individuals/organisations and Council and may prevent future breaches.

3.3 To support Council's obligations under the PPIP Act, and to promote robust and effective privacy, data handling and information governance procedure, Council also has a Data Breach Procedure. The Procedure outlines the steps for managing a data breach, including providing examples of situations that will be considered an eligible data breach, the steps involved in responding to a data breach, and the considerations around notifying persons whose privacy may be affected by the breach.

3.4 This Policy should be read in conjunction with Council's Privacy Management Plan which provides more information on how Council may collect, use, and disclose personal information and the Data Breach Procedures.

4. WHAT IS AN ELIGIBLE DATA BREACH?

4.1 A data breach occurs when personal information held by Council (whether held in digital or hard copy) is subject to unauthorised access, unauthorised disclosure or is lost in circumstances where the loss is likely to result in unauthorised access or unauthorised disclosure.

4.2 Under the Notifiable Data Breaches (NDB) Scheme, any organisation or agency covered by the Privacy Act must notify individuals and the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved.

4.3 For Council, it is mandatory to apply the NDB Scheme to tax file numbers it holds.

4.4 This may or may not involve disclosure of personal information external to Council or publicly. For example, unauthorised access to personal information by a Council employee, or unauthorised sharing of personal information between teams within Council may amount to a data breach.

4.5 A data breach may occur as the result of malicious action, system failure or human error. A data breach may also occur because of a misconception about whether a particular act or practice is permitted under the Information Protection Principles (IPPs).

4.6 Examples include:

Human error

- When a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information is lost or misplaced.
- When system access is incorrectly granted to someone without appropriate authorisation.
- When staff fail to implement appropriate password security, for example, not securing passwords or sharing password and login details.
- When a letter or document is posted to an incorrect address; or an email is sent to an incorrect recipient; or information is published on Council's website without consent.

System failure

- When a coding error allows access to a system without authentication, or results in automatically generated notices including the wrong information or being sent to incorrect recipients.
- Where systems are not maintained through the application of known and supported patches.

Malicious or criminal attack

- Cyber incidents such as ransomware, malware, hacking, phishing or brute force access attempts resulting in access to or theft of personal information.
- Social engineering or impersonation leading to inappropriate disclosure of personal information.
- Insider threats from Council employees using their valid credentials to access or disclose personal information outside the scope of their duties or permissions.
- Theft of a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information.

4.7 The MNDB Scheme applies where an eligible data breach has occurred. For a data breach to constitute an eligible data breach under the MNDB Scheme, there are two tests to be satisfied:

- There is an unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency or there is a loss of personal information held by a public sector agency in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of, the information; and
- A reasonable person would conclude that the access or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates.

Meaning of 'serious harm'

4.8 The term 'serious harm' is not defined in the PPIP Act. Harms that can arise as a result of a data breach are context-specific and will vary based on:

- The type of personal information accessed, disclosed or lost, and whether a combination of different types of personal information might lead to increased risk;
- The level of sensitivity of the personal information accessed, disclosed or lost;
- The amount of time the information was exposed or accessible, including the amount of time information was exposed prior to the agency discovering the breach;
- The circumstances of the individuals affected and their vulnerability or susceptibility to harm (that is, if any individuals are at heightened risk of harm or have decreased capacity to protect themselves from harm);
- The circumstances in which the breach occurred; and
- Actions taken by Council to reduce the risk of harm following the breach.

4.9 Serious harm occurs where the harm arising from the eligible data breach has, or may, result in a real and substantial detrimental effect to the individual. The effect on the individual must be more than mere irritation, annoyance or inconvenience.

4.10 Harm to an individual includes physical harm; economic, financial or material harm; emotional or psychological harm; reputational harm; and other forms of serious harm that a reasonable person in Council's position would identify as a possible outcome of the data breach.

5. SYSTEMS AND PROCESSES FOR MANAGING DATA BREACHES

5.1 Council has established and implemented a comprehensive set of controls, measures and processes for preventing, responding to and managing data breaches.

5.2 This includes projects to increase cyber security maturity, cyber security training for all staff, robust access controls, and network and endpoint security measures and data loss prevention systems.

5.3 An up-to-date inventory of assets is maintained, and strong patch and vulnerability management measures to ensure all IT assets are properly secured and monitored. Regular penetration tests are performed to identify and remediate any weaknesses in the IT infrastructure.

5.4 Council will ensure all third-party providers who store personal and health information on behalf of Council are aware of the MNDB Scheme and the obligations under this Policy to report any eligible data breaches to the IPC.

5.5 Council also has a range of policies and procedures to prevent, control and mitigate exposures to breaches of data, including its Code of Conduct and the Privacy Management Plan

5.6 To mitigate the risk of data breaches, Council regularly conducts awareness training to educate employees about the risks associated with data breaches, and their responsibilities as a public official to recognise, respond, report and prevent such incidents.

5.7 Council also maintains an internal register for data breaches and has implemented recommended changes to systems and policies in response to reviewing the causes of data breaches to assist in preventing future breaches.

6. RESPONDING TO A DATA BREACH

6.1 Each data breach is unique and will require a tailored response. The response actions will depend on several factors, including the type of data compromised, the cause of the breach and the potential harms that could arise for affected individuals.

6.2 While the details of each breach will be different, the process for responding to a data breach is the same and will be followed in each instance to ensure a consistent approach.

6.3 In line with the recommendations from the IPC, Council will follow the below steps when investigating and responding to a data breach:

- Initial report and triage;
- Contain the breach;
- Assess and mitigate;
- Notify; and
- Review.

6.4 The full procedure for investigation of a data breach is set out in the Data Breach Procedures.

7. RESPONSIBILITIES

Compliance, monitoring and review

7.1 The following staff have identified roles under this Policy:

Information Services Manager

The Information Services Manager is responsible for:

- implementing this Policy,
- reporting data breaches to the General Manager and all notifications and actions for eligible data breaches
- Assisting the Director Corporate and Community Services with investigations.
- for notifying the Privacy Commissioner after an eligible data breach is identified.
- maintaining the internal and public registers for data breaches.
- preparing the Data Breach Report and Action Plan.
- is responsible for preparing an annual report to Council's Executive Leadership Team on the number and nature of data breach incidents within Council.

General Manager (or their delegate)

The General Manager (or their delegate) will determine the method and oversee the notification of any affected individuals of a data breach, including eligible data breaches under the MNDB Scheme.

Director Corporate & Community Services

The Director Corporate & Community Services, in conjunction with the Information Services Manager, is responsible for investigating data breaches.

The Director Corporate & Community Service, in conjunction with the Coordinator Community Engagement will provide advice on the communication strategy, and messaging to affected individuals and external reporting agencies.

Governance Officer

The Governance Officer is responsible for monitoring and reviewing the type of data breaches (including those under the MNDB Scheme) to identify trends and areas of concern where staff may require additional training and systems and processes need to be remediated to prevent future incidents.

All Council Employees

All employees have a responsibility for immediately reporting a suspected data breach in accordance with this Policy and the Procedure.

7.2 This Policy will be reviewed, tested, and updated in accordance with Council's Policy Framework or as required by best practice or legislation.

7.3 Suspected breaches or misuse of this policy are to be reported to the General Manager. Alleged breaches of this policy shall be dealt with by the processes outlined for breaches of the Code of Conduct, as detailed in the Code of Conduct.

Reporting

7.4 Council will report all eligible data breaches in accordance with the MNDB Scheme and the PPIP Act.

7.5 An annual report will be provided to Council's Executive Leadership Team outlining the number and nature of data breach incidents within Council. This report may also be provided to Council's Audit, Risk and Improvement Committee where appropriate

Records management

7.6 Staff must maintain all records relevant to administering this Policy in accordance with Council's Records Management Policy

8. DEFINITIONS

Act	the Local Government Act 1993 (NSW)
Council	Lachlan Shire Council
Data Breach:	the unauthorised access to, or inadvertent disclosure, access, modification, use, misuse or loss of, or interference with Personal Information held by Council and in this Policy includes a potential Data Breach.
Personal Information	for the purposes of the MNDB Scheme means 'information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.' This also includes information about an individual's physical or mental health, disability and information connected to the provision of a health service.
Relevant Manager or Director	Manager or Director to whom a Council Officer responsible for the data subject to the breach reports or Director with responsibility for a contract with a third party
Affected individual	an affected individual as defined in the PPIP Act. Council Officer means any officer or employee of Council.

9. RELATED DOCUMENTS

Related LSC policies include

- Code of Conduct for Council Staff
- Code of Conduct for Councillors
- Privacy Management Plan

Related Legislation includes:

- Privacy & Personal Information Protection Act 1998 (PPIP Act)
- Mandatory Notification of Data Breach Scheme
- Health Records and Information Privacy Act 2002 (HRIP Act)
- Privacy Act 1988 (Cth) (Privacy Act)

Greg Tory

GENERAL MANAGER

LACHLAN SHIRE COUNCIL
Wiradjuri Country

LACHLAN SHIRE COUNCIL
DATA BREACH PROCEDURES

Table of Contents

1. PROCEDURE PURPOSE

1.1 The objectives of this Procedure is provide guidance and steps for staff to follow when responding to a breach of Lachlan Shire Council (Council) held data

2. SCOPE This Procedure applies to:

2.1.1 all staff and contractors of Council, including Councillors, students, volunteers, and third party providers who hold personal and health information on behalf of Council.

2.1.2 Council data held in any format (paper based or electronic). The Procedure does not apply to information that has been classified as public.

3. PROCEDURE STATEMENT

3.1 Council is committed to ensuring, as far as practicable, that the data it holds is secure from potential data breaches. Where a breach of that data does occur, it is essential that there are appropriate steps in place to ensure quick and appropriate action is taken.

3.2 Having a data breach policy and procedure is part of Council's privacy and information governance procedures and framework. Effective breach management assists Council in avoiding or reducing possible harm to both affected individuals or organisations and Council and may prevent future breaches.

3.3 This Procedure should be read in conjunction with Council's Privacy Management Plan which provides more information on how Council may collect, use and disclose personal information as well as the Data Breach Policy

4. REPORTING AND RESPONDING TO A DATA BREACH

4.1 Council's response to a data breach will be undertaken promptly to enable Council to contain, assess and respond to data breaches efficiently, as well as to help minimise harm to affected individuals.

4.2 There are five key steps required in responding to a data breach or suspected data breach:

4.2.1 Initial report and triage;

4.2.2 Contain the breach;

4.2.3 Assess and mitigate;

4.2.4 Notify; and

4.2.5 Review.

4.3 The first four steps should be carried out concurrently where possible. The last step provides recommendations for longer-term solutions and prevention strategies.

4.4 The Information Services Manager must be informed of any data breach or suspected data breach to ensure Council meets its legislative obligations, including notifying the Privacy Commissioner for eligible data breaches and affected individuals and the Office of the Australian Information Commissioner (OAIC) as required.

4.5 Where appropriate, the Director Corporate & Community Services will ensure that appropriate advice and information is provided to relevant Council staff to assist in responding to any enquiries made by the public, preparing appropriate communications and managing complaints that may be received as a result of the data breach.

4.6 Each step is set out in further detail below:

Step 1: Initial report and triage

4.6.1 Any staff member, contractor or third-party provider who becomes aware of a data breach or becomes aware that are grounds to suspect a data breach is to notify the Information Services Manager or the Governance and Risk Officer immediately and provide details of the breach.

4.6.2 The Information Services Manager or their delegate will review the information provided and notify the General Manager (or their delegate) of any eligible data breach.

4.6.3 Council may also convene a Data Breach Response Team where a data breach involves highly sensitive information, has a high risk of harm to individuals and affects more than one individual.

Step 2: Contain the breach

4.6.4 Containment of the breach is prioritised by Council and all necessary steps possible must be taken to contain the breach and minimising any resulting damage. This obligation is ongoing as the other steps proceed.

4.6.5 Examples of containment methods may include:

- Stop any unauthorised practice(s) and suspend the activity that led to the breach;
- Recover any records or personal information;
- Shut down the system that was breached (if practicable); and/or
- Revoke or change the account privileges or change access codes or passwords.

4.6.6 If a third party is in possession of the data and refuses to return it, it may be necessary for Council to seek legal or other advice on what action can be taken to recover the data.

4.6.7 When recovering data, Council will make sure that copies that have not been made by a third party or, if they have, that all copies are recovered. This can include receiving written confirmation from a third party that the copy of the data that they received in error has been permanently deleted.

Step 3: Assess and mitigate

4.6.8 Council will undertake an assessment of the type of data involved in the breach, whether the breach is an eligible breach under the MNDB Scheme and the risks and potential for serious harm associated with the breach.

4.6.9 The Data Breach Report and Action Plan will be used for reporting on the investigation of the breach and authorising actions in response. The Governance and Risk Officer will prepare a report and provide to the Information Services Manager who will review the proposed actions and recommendations of the report prior to the Report being provided to the General Manager for approval.

4.6.10 Data Breach Report and Action Plans are to be saved in in the appropriate folder in Council's electronic record keeping system. (17.11.2.1).

4.6.11 The Information Services Manager will be responsible for the implementation of proposed actions and recommendations.

4.6.12 After a suspected data breach is reported to the General Manager or their delegate, an assessment must be carried out within 30 days to determine whether there are reasonable grounds to believe that the suspected data breach is an eligible data breach. This date may be subject to an extension in accordance with the PPIP Act.

4.6.13 thorough evaluation of the risks will assist Council in determining the appropriate course of action to take. The factors that may be considered (but are not limited to) when assessing the breach include:

- The type of information is involved in the breach
- The sensitivity of the personal information involved in the breach;
- Whether the personal information is or was protected by security measures;
- The persons to whom the unauthorised access to, or unauthorised disclosure of, the personal information involved in the breach was, or could be, made or given,
- The likelihood of the persons who has received or has access to the personal information has or had the intention of causing harm or could or did circumvent security measures protecting the information;
- The nature of the harm that has or may occur; and
- Other matters specified in guidelines issued by the Privacy Commissioner about whether the disclosure is likely to result in serious harm to an individual to whom the personal information relates.

4.6.14 Further actions may include interviews (or further interviews) with staff involved and/or affected, or the request of further investigation by appropriate Council staff into system failures or IT security issues.

4.6.15 During the assessment, the General Manager must make all reasonable attempts to mitigate the harm done by the suspected breach.

4.6.16 To mitigate the breach, Council will consider the following measures:

- Implementation of additional security measures within Council's own systems and processes to limit the potential for misuse of compromised information.
- Limiting the dissemination of breached personal information. For example, by scanning the internet to determine whether the lost or stolen information has been published and seeking its immediate removal from public sites.
- Engaging with relevant third parties to limit the potential for breached personal information to be misused for identity theft or other purposes, or to streamline the re-issue of compromised identity documents. For example, contacting an identity issuer or financial institution to advise caution when relying on particular identity documents for particular cohorts.

Step 4: Notify

4.6.17 If an eligible data breach has occurred, the notification process under the MNDB Scheme is triggered. There are four elements of the notification process:

- The General Manager (or their delegate) will immediately notify the Privacy Commissioner after an eligible data breach is identified using the approved form as published on the IPC's website.
- Determine whether an exemption to notification applies. If one of the six exemptions set out in Division 4 of the MNDB Scheme applies in relation to an eligible data breach, Council may not be required to notify affected individuals.
- If an exemption does not apply, notify affected individuals or their authorised representatives as soon as practicable; and.
- Provide any further information to the Privacy Commissioner.

4.6.18 The General Manager (or their delegate) and the Response Team (if appointed) will determine how to notify, and oversee the notification to, affected individuals of the eligible data breach in accordance with this Procedure and the PPIP Act.

4.6.19 If a data breach is not an eligible data breach under the MNDB Scheme, Council may still consider notifying individuals/organisations of the breach, dependent on the type of information that is involved, the risk of harm, repeated and/or systematic issues and the ability of the individual/organisation to take further steps to avoid or remedy harm.

4.6.20 The method of notifying affected individuals/organisations will depend in large part on the type and scale of the breach, as well as immediately practical issues such as having contact details for the affected individuals/organisations.

4.6.21 Considerations include the following:

When to notify

4.6.22 Individuals/organisations affected by a data breach will be notified as soon as reasonably practicable. While this Procedure sets a target of 5 days; practical factors are also recognised. Where all individuals affected by an eligible data breach cannot be notified, Council will consider issuing a public notification on its website.

How to notify

4.6.23 Notification should be direct either by phone, letter, email or in person, to the affected individuals/organisations.

4.6.24 Indirect notification, such as information posted on Council's website, posted notices or media releases should only occur where direct notification could cause further harm, is cost prohibitive or the contact information for affected individuals/organisations is unknown. The General Manager can also determine to issue a public notification if it is appropriate.

4.6.25 A record of any public notification of a data breach will be published on Council's website and recorded on the Public Data Breach Register for a period of 12 months.

What to say

4.6.26 The following information must, if reasonably practicable, be included in a notification to an affected individual of a data breach:

- The date the breach occurred;
- A description of the breach;
- How the breach occurred;
- The type of breach that occurred;
- The personal information included in the breach;
- The amount of time the personal information was disclosed for;

- Actions that have been taken or are planned to secure the information, or to control and mitigate the harm;
- Recommendations about the steps an individual should take in response to the breach;
- Information about complaints and reviews of agency conduct;
- The name of the agency or agencies that were subject to the breach;

4.6.27 Contact details for the agency subject to the breach or the nominated person to contact about the breach. Other obligations including external engagement or reporting

4.6.28 Council will also consider whether notification is required by contract or by other laws or administrative arrangements to take specific steps in response to a data breach. These may include taking specific containment or remediation steps or engaging with or notifying external stakeholders (in addition to the Privacy Commissioner) where a data breach occurs.

4.6.29 Depending on the circumstances of a data breach, such as an intentional or suspected serious data breach and the categories of data involved, it may be appropriate to notify other agencies/third parties, such as:

- The OAIC, where a data breach may involve agencies under Federal jurisdiction;
- The NSW Police Force and/or Australian Federal Police, where Council suspects a data breach is a result of criminal activity;
- Cyber Security NSW, where a data breach is a result of a cyber-security incident;
- The Australian Cyber Security Centre, where a data breach involves malicious activity from a person or organisation based outside Australia;
- Council's insurance providers;
- Credit card companies, financial institutions/services providers;
- Professional associations, regulatory bodies or insurers, where a data breach involves malicious activity from a person or organisation outside Australia; and/or
- Other internal or external parties who have not already been notified.

4.6.30 Any reported incidents of suspected misconduct must also be reported to Council's Disclosures Coordinator as soon as practicable.

4.6.31 Where a data breach is subject to the NDB Scheme (which for Council is currently limited with respect to tax files numbers), Council must promptly notify individuals at likely risk of serious harm as well as the OAIC. The notification must include:

- Information identifying Council and its contact details;
- A description of the data breach;
- The kinds of information concerned; and
- Recommendations about the steps that individuals should take in response to the data breach.

4.6.32 The General Manager (or their delegate) and the Response Team (if appointed) will determine how to notify and oversee the notification made to the OAIC and any affected individuals of the MNDB Scheme data breach.

4.6.33 Council may become subject to other legislation relevant to data breaches impacting on other agencies. For example, under the Data Sharing (Government Sector) Act 2015:

- If Council is the recipient of data from another NSW Government agency that contains personal information or health information, and
- Council becomes aware that the Privacy and Personal Information Protection Act 1998 or the Health Records and Information Privacy Act 2002 has been or is likely to be contravened in relation to that information while in Council's control
- In such instances, Council must inform the other agency and the NSW Privacy Commissioner of the contravention as soon as practicable after becoming aware of it.

Step 5: Review

4.6.35. Council must ensure that the cause of the breach has been fully investigated, and that the appropriate people have been briefed on outcomes and recommendations. This includes investigating the circumstances of data breaches to determine all relevant causes and consider what short or long-term measures can be taken to prevent any reoccurrence.

4.6.36. Depending on the nature of the breach, this step may be completed as part of the assessment of the first four steps and mitigation of the breach as detailed in step 3 above.

4.6.37. Preventative actions could include:

- Review of Council's IT systems and remedial actions to prevent future data breaches;
- Security audit of both physical and technical security controls
- Review of policies and procedures
- Review of staff/contractor training practices e) Review of contractual obligations with contracted service providers.

4.6.38. At a minimum, amendments to relevant policies and procedures should be made where necessary, and staff training should be undertaken where deemed appropriate.

4.6.39. A debriefing session should be held with relevant staff to assess the cause of and response to the breach, and to ensure any necessary recommendations are allocated and actioned appropriately.

4.6.40. Any recommendations to implement the above preventative actions are to be approved by the General Manager and documented in Council's electronic record keeping system.

4.6.41. Consideration will be given to reporting relevant matters to Council's Audit, Risk and Improvement Committee and to Council. '

Data Retention

4.6.42. When a data breach incident is being investigated, all records are to be documented and recorded in Council's electronic record keeping system, including all related documents and supporting evidence of a breach.

5. RESPONSIBILITIES

Compliance, monitoring and review

5.1 The following staff have identified roles under this Procedure:

The Information Services Manager is responsible for:

- implementing this Policy,
- reporting data breaches to the General Manager and all notifications and actions for eligible data breaches
- Assisting the Director Corporate and Community Services with investigations.
- for notifying the Privacy Commissioner after an eligible data breach is identified.
- maintaining the internal and public registers for data breaches.
- preparing the Data Breach Report and Action Plan.
- is responsible for preparing an annual report to Council's Executive Leadership Team on the number and nature of data breach incidents within Council.

General Manager (or their delegate)

The General Manager (or their delegate) will determine the method and oversee the notification of any affected individuals of a data breach, including eligible data breaches under the MNDB Scheme.

Director Corporate & Community Services

The Director Corporate & Community Services, in conjunction with the Information Services Manager, is responsible for investigating data breaches.

The Director Corporate & Community Service, in conjunction with the Coordinator Community Engagement will provide advice on the communication strategy, and messaging to affected individuals and external reporting agencies.

Governance Officer

The Governance Officer is responsible for monitoring and reviewing the type of data breaches (including those under the MNDB Scheme) to identify trends and areas of concern where staff may require additional training and systems and processes need to be remediated to prevent future incidents.

All Council Employees

5.1.1 All employees have a responsibility for immediately reporting a suspected data breach in accordance with this Procedure and the associated Policy.

5.2 This Procedure will be reviewed, tested and updated in accordance with Council's Policy Framework or as required by best practice or legislation.

6. REPORTING

6.1 Council will report all eligible data breaches in accordance with the MNDB Scheme and the Privacy and Personal Information Protection Act 1998 (PPIP Act). An annual report will be provided Council's Executive Leadership Team outlining the number and nature of data breach incidents within Council. This report may also be provided to Council's Audit, Risk and Improvement Committee where appropriate.

7. RECORDS MANAGEMENT

7.1 Staff must maintain all records relevant to administering this guideline in accordance with Council's Records Management Policy.

8. APPENDIX 1: DATA BREACH REPORT AND ACTION PLAN

Description of Data Breach	When?	
	What?	
	How?	
Action taken	Notification	
	Containment	
Description of risks	Risk?	
	Harm?	
	Affecting?	
Description of causes	How?	
	Why?	
	Is this a Systematic issue?	
Action Proposed	Change?	
	Train?	
	Remind?	
	Stop?	
	Media?	
	Remedy?	
	Other matters?	
Notification to Privacy Commissioner		

Australian Government
Office of the Australian Information Commissioner

Data breach preparation and response

A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)

oaic.gov.au

OAIC

Published: February 2018. Updated: July 2019.

Foreword

Strong data management is integral to the operation of businesses and government agencies worldwide. Digital platforms and technologies that utilise user data to provide personalised products or services have proliferated across communities and industries. At the same time, data analysis has been widely recognised for its value as fuel for innovation that can benefit the community in unprecedented ways, including identifying gaps in services, revealing needs for new or different products, and enabling better-informed policy-making.

In this environment, the success of an organisation that handles personal information or a project that involves personal information depends on trust. People have to trust that their privacy is protected, and be confident that personal information will be handled in line with their expectations.

As we've found in our long-running national community attitudes to privacy survey, if an organisation does not demonstrate a commitment to privacy, people will look for alternative suppliers, products, and services.

One of the biggest risks organisations face in this context is a data breach. A data breach involving personal information can put affected individuals at risk of serious harm and consequently damage an organisation's reputation as a data custodian.

However, it is important to recognise that consumer and community trust is not necessarily extinguished immediately after a data breach occurs. After all, history has shown us that even organisations with great information security can fall victim to a data breach, due to the rapid evolution of data security threats and the difficulty of removing the risk of human error in large and complex organisations.

When a data breach occurs, a quick and effective response can have a positive impact on people's perceptions of an organisation's trustworthiness. That is why being prepared for a data breach is important for all organisations that handle personal information.

By an 'effective' response to a data breach, I mean a response that successfully reduces or removes the risk of harm to individuals, and which aligns with legislative requirements and community expectations.

This guide aims to assist you in developing and implementing an effective data breach response. It outlines the requirements relating to data breaches in the Privacy Act 1988 (Cth) (Privacy Act), including personal information security requirements and the mandatory data breach reporting obligations of the Notifiable Data Breaches (NDB) scheme. The guide also covers other key considerations in developing a robust data breach response strategy, including the key steps to take when a breach occurs, the capabilities of staff, and governance processes.

While this guide is primarily for Australian Government agencies and private sector organisations with obligations under the Privacy Act, the information provided is useful to any organisation operating in Australia. Taken holistically, the information provided in this guide provides a framework for meeting expectations for accountability and transparency in data breach prevention and management, which is key to maintaining and building consumer and community trust.

Timothy Pilgrim PSM

Australian Information Commissioner
Australian Privacy Commissioner

Contents

Purpose and structure of this guide

The Office of the Australian Information Commissioner (OAIC) has prepared this guide to assist Australian Government agencies and private sector organisations (entities) prepare for and respond to data breaches in line with their obligations under the Privacy Act 1988 (Cth) (Privacy Act).

The guide is in five parts.

Part 1: Data breaches and the Australian Privacy Act

This section outlines the requirements of the Privacy Act that relate to personal information security and data breach response strategy. The principles contained within the Privacy Act for the handling of personal information may be adopted by any entity to lower the risk of a data breach occurring and to effectively reduce the impact of a data breach.

Part 2: Preparing a data breach response plan

The faster an entity responds to a data breach, the more likely it is to effectively limit any negative consequences. A data breach response plan is essential to facilitate a swift response and ensure that any legal obligations are met following a data breach.

Part 3: Responding to data breaches — Four key steps

An effective data breach response generally follows a four-step process — contain, assess, notify, and review. This section outlines key considerations for each of these steps to assist entities in preparing an effective data breach response.

Part 4: Notifiable Data Breaches

This section outlines the requirements of the NDB scheme under the Privacy Act. The NDB scheme contains mandatory data breach reporting obligations in relation to certain data breaches, and requirements to assess suspected data breaches.

Part 5: Other sources of information

The obligations of the Privacy Act in relation to data breaches co-exist with other reporting obligations. This section assists entities in identifying where they can find information about other data breach reporting requirements.

Who should use this guide?

Any entity that handles personal information can use this guide to inform their preparation and response strategy for a data breach.

However, this guide is primarily targeted at entities that have obligations under the Privacy Act to protect personal information. These entities are required to take reasonable steps to protect the personal information that they hold, and may be required to notify affected individuals and the Australian Information Commissioner (Commissioner) of a data breach under the NDB scheme.

How to use this guide

Different parts of this guide will be of greater or lesser relevance to different entities depending on their goals.

Entities seeking a greater understanding of the Privacy Act, specifically in how the Privacy Act's requirements relate to personal information security and data breach management responsibilities, should refer primarily to Part 1 and Part 4.

Entities that want to prepare a data breach response strategy, or review the effectiveness of their current response plan, should refer primarily to Part 2 and Part 3.

Entities that have experienced a data breach can refer to Part 3 to understand the main components of an effective data breach response. They should also refer to Part 4, as it provides guidance on the mandatory data breach reporting and assessment requirements of the NDB scheme.

A cautionary note

There is no 'one size fits all' solution to preparing for and responding to data breaches. This guide does not provide detailed information about the systems or processes an entity may put in place to manage data breaches.

Further, this guide does not provide detailed information about other obligations that may apply to entities in addition to the Privacy Act. Entities should consider their privacy obligations alongside other relevant legal requirements and standards.

The guide does not constitute or replace legal advice on obligations under the Privacy Act. It is published by the Commissioner to provide general information to help entities meet the requirements of the Privacy Act. Entities are encouraged to seek professional advice tailored to their own circumstances where required.

Part 1: Data breaches and the Australian Privacy Act

Key points

- A data breach is an unauthorised access or disclosure of personal information, or loss of personal information.
- Data breaches can have serious consequences, so it is important that entities have robust systems and procedures in place to identify and respond effectively.
- Entities that are regulated by the Privacy Act should be familiar with the requirements of the NDB scheme, which are an extension of their information governance and security obligations.
- A data breach incident may also trigger reporting obligations outside of the Privacy Act.

What is a data breach?

A data breach occurs when personal information that an entity holds is subject to unauthorised access or disclosure, or is lost.

Personal information is information about an identified individual, or an individual who is reasonably identifiable.[1] Entities should be aware that information that is not about an individual on its own can become personal information when it is combined with other information, if this combination results in an individual becoming 'reasonably identifiable' as a result.

A data breach may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems.

Examples of data breaches include:

- loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information
- unauthorised access to personal information by an employee
- inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person
- disclosure of an individual's personal information to a scammer, as a result of inadequate identity verification procedures.

Consequences of a data breach

Data breaches can cause significant harm in multiple ways.

[1] Section 6 of the Privacy Act. For detailed information about the scope of 'personal information', see What is personal information?, OAIC website <https://www.oaic.gov.au>.

Individuals whose personal information is involved in a data breach may be at risk of serious harm, whether that is harm to their physical or mental well-being, financial loss, or damage to their reputation.

Examples of harm include:

- financial fraud including unauthorised credit card transactions or credit fraud
- identity theft causing financial loss or emotional and psychological harm
- family violence
- physical harm or intimidation.

A data breach can also negatively impact an entity's reputation for privacy protection, and as a result undercut an entity's commercial interests. As shown in the OAIC's long-running national community attitudes to privacy survey, privacy protection contributes to an individual's trust in an entity.[2] If an entity is perceived to be handling personal information contrary to community expectations, individuals may seek out alternative products and services.

An entity can reduce the reputational impact of a data breach by effectively minimising the risk of harm to affected individuals, and by demonstrating accountability in their data breach response. This involves being transparent when a data breach, which is likely to cause serious harm to affected individuals, occurs. Transparency enables individuals to take steps to reduce their risk of harm. It also demonstrates that an entity takes their responsibility to protect personal information seriously, which is integral to building and maintaining trust in an entity's personal information handling capability.

The Australian Privacy Principles

The Privacy Act contains 13 Australian Privacy Principles (APPs) that set out entities' obligations for the management of personal information. The APPs are principles-based and technologically neutral; they outline principles for how personal information is handled and these principles may be applied across different technologies and uses of personal information over time.

Compliance with the APPs as a whole will reduce the risk of a data breach occurring. This is because the APPs ensure that privacy risks are reduced or removed at each stage of personal information handling, including collection, storage, use, disclosure, and destruction of personal information. For example, APP 3 restricts the collection of personal information. APPs 4.3 and 11.2 outline requirements to destroy or de-identify information if it is unsolicited or no longer needed by the entity. Compliance with these requirements reduces the amount of data that may be exposed as a result of a breach.

Compliance with the requirement to secure personal information in APP 11 is key to minimising the risk of a data breach.[3] APP 11 requires entities to take reasonable steps to protect the personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. The type of steps that are reasonable to protect information will

---

[2] See the Australian Community Attitudes to Privacy surveys at Research, OAIC website <https://www.oaic.gov.au>.

[3] Sections 20Q and 21S of the Privacy Act impose equivalent obligations on credit reporting agencies and all credit providers. Similarly, the Privacy (Tax File Number) Rule 2015 <https://www.legislation.gov.au/Details/F2015L00249> made under s 17 of the Privacy Act requires TFN recipients to take reasonable steps to protect TFN information from misuse and loss, and from unauthorised access, use, modification or disclosure.

depend on the circumstances of the entity and the risks associated with personal information handled by the entity.[4]

In addition, APP 1 requires entities to take reasonable steps to establish and maintain practices, procedures, and systems to ensure compliance with the APPs.[5]

The OAIC has published various resources to assist entities to meet their obligations under APP 1.2[6] and APP 11.[7]

The Notifiable Data Breaches (NDB) scheme

The NDB scheme in Part IIIC of the Privacy Act requires entities to notify affected individuals and the Commissioner of certain data breaches.

The NDB scheme requires entities to notify individuals and the Commissioner about 'eligible data breaches'. An eligible data breach occurs when the following criteria are met:

- There is unauthorised access to or disclosure of personal information held by an entity (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
- This is likely to result in serious harm to any of the individuals to whom the information relates.
- The entity has been unable to prevent the likely risk of serious harm with remedial action.

Entities must also conduct an assessment if it is not clear if a suspected data breach meets these criteria. The assessment will determine whether the breach is an 'eligible data breach' that triggers notification obligations.

The primary purpose of the NDB scheme is to ensure individuals are notified if their personal information is involved in a data breach that is likely to result in serious harm. This has a practical function: once notified about a data breach, individuals can take steps to reduce their risk of harm. For example, an individual can change passwords to compromised online accounts, and be alert to identity fraud or scams.

The NDB scheme also serves the broader purpose of enhancing entities' accountability for privacy protection. By demonstrating that entities are accountable for privacy, and that breaches of privacy are taken seriously, the NDB scheme works to build trust in personal information handling across industries.

Part 4 of this guide provides detailed information to assist entities to meet their obligations under Part IIIC of the Privacy Act when responding to an eligible data breach or a suspected eligible data breach.

---

[4] See Chapter 11 of the APP Guidelines and the Guide to Securing Personal Information on the OAIC website <https://www.oaic.gov.au>.

[5] A similar requirement applies to credit reporting bodies in s 20B(2), to take reasonable steps to implement practices, procedures and systems to ensure compliance with the credit reporting obligations in Part IIIA of the Privacy Act and the Privacy (Credit Reporting) Code 2014 (Version 2.1) <https://www.legislation.gov.au/Details/F2020L00126>.

[6] See Privacy Management Framework, Privacy Management Plan Template (for Organisations), Interactive Privacy Management Plan (for Agencies), and Chapter 1 of the APP Guidelines on the OAIC website <https://www.oaic.gov.au>.

[7] See Chapter 11 of the APP Guidelines and the Guide to Securing Personal Information on the OAIC website <https://www.oaic.gov.au>.

Other obligations

Entities may have other obligations outside of those contained in the Privacy Act that relate to personal information protection and responding to a data breach. These may include other data protection obligations under state-based or international data protection laws. Australian businesses may need to comply with the European Union's (EU's) General Data Protection Regulation (GDPR)[8] if they have an establishment in the EU, if they offer goods and services in the EU, or if they monitor the behaviour of individuals in the EU.

For data breaches affecting certain categories of information, other mandatory or voluntary reporting schemes may exist. For example, entities might consider reporting certain breaches to:

- the entity's financial services provider
- police or law enforcement bodies
- the Australian Securities & Investments Commission (ASIC)
- the Australian Prudential Regulation Authority (APRA)
- the Australian Taxation Office (ATO)
- the Australian Transaction Reports and Analysis Centre (AUSTRAC)
- the Australian Cyber Security Centre (ACSC)
- the Australian Digital Health Agency (ADHA)
- the Department of Health
- State or Territory Privacy and Information Commissioners
- professional associations and regulatory bodies
- insurance providers.

Other resources are listed in Part 5 of this guide.

Some entities may have additional obligations to report to the Commissioner under the National Cancer Screening Register Act 2016 (NCSR Act) or have different reporting obligations under the My Health Records Act 2012 (My Health Records Act).

Under the NCSR Act, current and former contracted service providers of the National Cancer Screening Register must notify the Secretary of the Department of Health (the Secretary) and the Commissioner if they become aware of unauthorised recording, use or disclosure of personal information included in the Register. The Secretary must also notify the Commissioner of certain data breaches, including potential breaches, in connection with the National Cancer Screening Register. The Secretary must also consult the Information Commissioner about notifying individuals who may be affected. Separately, entities with NCSR Act obligations must consider whether the incident also requires notification under the NDB scheme, as the two schemes operate concurrently. Where the test for both schemes have been met, the entity may make a joint notification to the Commissioner.

[8] The OAIC's Australian Entities and the EU General Data Protection Regulation may assist Australian businesses to understand and comply with the GDPR's requirements. Further guidance is also available from the Article 29 Working Group <http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360&tpa_id=6936>.

Certain participants in the My Health Record system (such as the System Operator, a registered healthcare provider organisation, a registered repository operator, a registered portal operator or a registered contracted service provider), are required to report data breaches that occur in relation to the My Health Record system to the either the System Operator or the Commissioner, or both, depending on the entity reporting the data breach (s 75 of the My Health Records Act). More information about obligations under the My Health Records Act and how these obligations interact with the NDB scheme is available in Part 4.

Part 2: Preparing a data breach response plan

Key points

- A quick response to a data breach, based on an up-to-date data breach response plan, is critical to effectively managing a breach
- your data breach response plan should outline your entity's strategy for containing, assessing and managing the incident from start to finish
- this part will provide practical guidance to help you develop a comprehensive and effective data breach response plan.

Why do you need a data breach response plan?

All entities should have a data breach response plan. A data breach response plan enables an entity to respond quickly to a data breach. By responding quickly, an entity can substantially decrease the impact of a breach on affected individuals, reduce the costs associated with dealing with a breach, and reduce the potential reputational damage that can result.

A data breach response plan can help you:

- **Meet your obligations under the Privacy Act**
  Under the Privacy Act, an entity must take reasonable steps to protect the personal information that it holds.[9] A data breach response plan focussed on reducing the impact of a breach can be one of these reasonable steps.
- **Limit the consequences of a data breach**
  A quick response can reduce the likelihood of affected individuals suffering harm. It can also lessen financial or reputational damage to the entity that experienced the breach.
- **Preserve and build public trust**
  An effective data breach response can support consumer and public confidence in an entity's respect for individual privacy, and the entity's ability to manage personal information in accordance with community expectations.

What is a data breach response plan?

A data breach response plan is a framework that sets out the roles and responsibilities involved in managing a data breach. It also describes the steps an entity will take if a data breach occurs.

Your data breach response plan should be in writing to ensure that your staff clearly understand what needs to happen in the event of a data breach. It is also important for staff to be aware of where they can access the data breach response plan on short notice.

---

[9] An APP entity is required under s 15 not to do an act, or engage in a practice, that breaches APP 11.1; a credit reporting body is required to comply with s 20Q in relation to credit reporting information; a credit provider is required to comply with s 21S(1) in relation to credit eligibility information; a file number recipient is required under s 18 not to do an act, or engage in a practice, that breaches the Privacy (Tax File Number) Rule 2015 <https://www.legislation.gov.au/Details/F2015L00249>.

You will need to regularly review and test your plan to make sure it is up to date and that your staff know what actions they are expected to take. You can test your plan by, for example, responding to a hypothetical data breach and reviewing how your response could be made more effective.

How regularly you test your plan will depend on your circumstances, including the size of your entity, the nature of your operations, the possible adverse consequences to an individual if a breach occurs, and the amount and sensitivity of the information you hold. It may be appropriate in some instances that a review of the plan coincides with the introduction of new products, services, system enhancements, or such other events which involve the handling of personal information.

What should the plan cover?

The more comprehensive your data breach response plan is, the better prepared your entity will be to effectively reduce the risks and potential damage that can result.

Information that your plan should cover includes:

- **A clear explanation of what constitutes a data breach**
  This will assist your staff in identifying a data breach should one occur (see What is a Data Breach? section above). You may also want to include potential examples of a data breach which are tailored to reflect your business activities.

- **A strategy for containing, assessing and managing data breaches**
  This strategy should include the actions your staff, and your response team, will take in the event of a data breach or a suspected data breach. Consider:
    - potential strategies for containing and remediating data breaches
    - ensuring you have the capability to implement those strategies as a matter of priority (e.g. having staff available to deal with the breach – see Response Team Membership section below). Your plan should reflect the capabilities of your staff to adequately assess data breaches and their impact, especially when breaches are not escalated to a response team
    - legislative or contractual requirements (such as the requirements of the NDB scheme if they apply to your entity)
    - a clear and immediate communications strategy that allows for the prompt notification of affected individuals and other relevant entities. In particular:
        - who is responsible for implementing the communications strategy
        - determining when affected individuals must be notified (refer to Identifying Eligible Data Breaches for further information about mandatory data breach notification requirements under the NDB scheme)
        - how affected individuals will be contacted and managed
        - criteria for determining which external stakeholders should be contacted (for example, law enforcement and cyber security agencies, regulators such as the OAIC, and the media)
        - who is responsible for liaising with external stakeholders.

- **The roles and responsibilities of staff**
  Your plan should outline the responsibilities of staff members when there is a data breach, or a suspected data breach. Consider:
  - who staff should inform immediately if they suspect a data breach
  - the circumstances in which a line manager can handle a data breach, and when a data breach must be escalated to the response team. The following factors may determine when a data breach is escalated to the response team:
    - the number of people affected by the breach or suspected breach
    - whether there is a risk of serious harm to affected individuals now or in the future
    - whether the data breach or suspected data breach may indicate a systemic problem with your entity's practices or procedures
    - other issues relevant to your circumstances, such as the value of the data to you or issues of reputational risk.
  - who is responsible for deciding whether the breach should be escalated to the response team. One option is for each senior manager to hold responsibility for deciding when to escalate a data breach to the response team. Another option is to have a dedicated role, such as the privacy contact officer.
- **Documentation**
  Your plan should consider how your entity will record data breach incidents, including those that are not escalated to the response team. This will assist you in ensuring you have documentation of how your entity has met regulatory requirements.
- **Review**
  Evaluating how a data breach occurred, and the success of your response, can help you improve your data handling and data breach management. Consider:
  - a strategy to identify and address any weaknesses in data handling that contributed to the breach
  - a system for a post-breach assessment of your entity's response to the data breach and the effectiveness of your data breach response plan.

Response team membership

Your data breach response team is responsible for carrying out the actions that can reduce the potential impact of a data breach. It is important that the staff that make up the response team, as well as their roles and responsibilities, are clearly established and documented before a data breach occurs. Otherwise, your response to the breach may be unnecessarily delayed.

Who is in your data breach response team will depend on the circumstances of your entity and the nature of the breach. Different skill sets and staff may be needed to respond to one breach compared to another. In some cases, you may need to include external experts in your team, for example legal advice, data forensics, or media management. You should identify the types of expertise you may need and ensure that this expertise will be available on short notice. You might consider creating a core team and adding other members as they are required.

You should keep a current list of response team members and clearly detail their roles, responsibilities, and authorities, as well as their contact details (possibly attached to the data breach response plan). You should ensure these contact details remain updated, particularly in the event of organisational changes. Each role on the response team should have a second point of contact in case the first person is not available.

Typical data breach response team roles and skills

Your data breach response team may include:

- a team leader — who is responsible for leading the response team and reporting to senior management
- a project manager — to coordinate the team and provide support to its members
- a senior member of staff with overall accountability for privacy and/or key privacy officer — to bring privacy expertise to the team
- legal support — to identify legal obligations and provide advice
- risk management support — to assess the risks from the breach
- Information and Communication Technology (ICT) support/forensics support — this role can help establish the cause and impact of a data breach that involved ICT systems
- information and records management expertise – to assist in reviewing security and monitoring controls related to the breach (for example, access, authentication, encryption, audit logs) and to provide advice on recording the response to the data breach
- human resources (HR) support — if the breach was due to the actions of a staff member
- media/communications expertise — to assist in communicating with affected individuals and dealing with the media and external stakeholders.

If you hold an insurance policy for data breaches, that insurer may have a pre-established panel of external service providers in many of the roles listed above. You may want to consult with your insurer as to the identity of that panel so they can be included in any response team. Alternatively, the insurer may have a hotline available to assist in the event of a data breach, and that could be noted in the response plan.

Which individuals carry out the roles outlined in your response team will depend on your circumstances. For example, in smaller entities it may not be necessary to include steps related to escalating the data breach to the response team, as this may be an automatic process. Depending on the size of your entity or the size of the breach, a single person may perform multiple roles. In smaller entities the owner/principal of the entity could potentially be the person who needs to respond to and act on that breach.

It is important that the response team has the authority to take the steps outlined in the response plan without needing to seek permission, as this will enable a faster response to the breach. The role of team leader should be carefully considered, as they should have sufficient ability and authority to effectively manage the various sections within the entity whose input is required and to report to senior management. It may be your senior member of staff with overall accountability for privacy, a senior lawyer (if you have an internal legal function) or another senior manager. If the breach is serious, it may be a senior executive.

Actions the response team should take

A data breach response plan should also set out (or refer to) the actions the response team is expected to take when a data breach is discovered. Part 3 of this Guide provides a general framework for responding to a data breach, and Part 4 outlines the requirements of the NDB scheme, which may apply to your entity if they have personal information security obligations under the Privacy Act.

The response team will need to consider what information needs to be reported to senior management and at what point. This reporting structure should form part of the plan.

The data breach response plan should outline how staff will record how they have become aware of a data breach and the actions taken in response. Keeping records on data breaches and suspected breaches will help you manage the breach and identify risks that could make a breach more likely to occur.

Other considerations

In developing your plan you could also consider:

- when and how the response team could practice a response to a breach in order to test procedures and refine them
- whether your plan for dealing with personal information data breaches could link into or be incorporated into already existing processes, such as a disaster recovery plan, a cyber security/ICT incident response plan, a crisis management plan or an existing data breach response plan involving other types of information (e.g. commercially confidential information)
- whether senior management should be directly involved in the planning for dealing with data breaches and in responding to serious data breaches
- any reporting obligations under laws other than the Privacy Act or to other entities
- whether you have an insurance policy for data breaches that includes steps you must follow.

Data breach response plan quick checklist

Use this list to check whether your response plan addresses relevant issues.

Information to be included	Yes/No	Comments
What a data breach is and how staff can identify one		
Clear escalation procedures and reporting lines for suspected data breaches		
Members of the data breach response team, including roles, reporting lines and responsibilities		
Details of any external expertise that should be engaged in particular circumstances		
How the plan will apply to various types of data breaches and varying risk profiles with consideration of possible remedial actions		
An approach for conducting assessments		
Processes that outline when and how individuals are notified		
Circumstances in which law enforcement, regulators (such as the OAIC), or other entities may need to be contacted		
Processes for responding to incidents that involve another entity		
A record-keeping policy to ensure that breaches are documented		
Requirements under agreements with third parties such as insurance policies or service agreements		
A strategy identifying and addressing any weaknesses in data handling that contributed to the breach		
Regular reviewing and testing of the plan		
A system for a post-breach review and assessment of the data breach response and the effectiveness of the data breach response plan		

Part 3: Responding to data breaches — Four key steps

Key points

- Each data breach response needs to be tailored to the circumstances of the incident.
- In general, a data breach response should follow four key steps: contain, assess, notify and review.

Overview

Data breaches can be caused or exacerbated by a variety of factors, involve different types of personal information, and give rise to a range of actual or potential harms to individuals and entities.

As such, there is no single way of responding to a data breach. Each breach will need to be dealt with on a case-by-case basis, with an understanding of the risks posed by a breach and the actions that would be most effective in reducing or removing these risks.

Generally, the actions taken following a data breach should follow four key steps:

Step 1: Contain the data breach to prevent any further compromise of personal information.

Step 2: Assess the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm.

Step 3: Notify individuals and the Commissioner if required. If the breach is an 'eligible data breach' under the NDB scheme, it may be mandatory for the entity to notify.

Step 4: Review the incident and consider what actions can be taken to prevent future breaches.

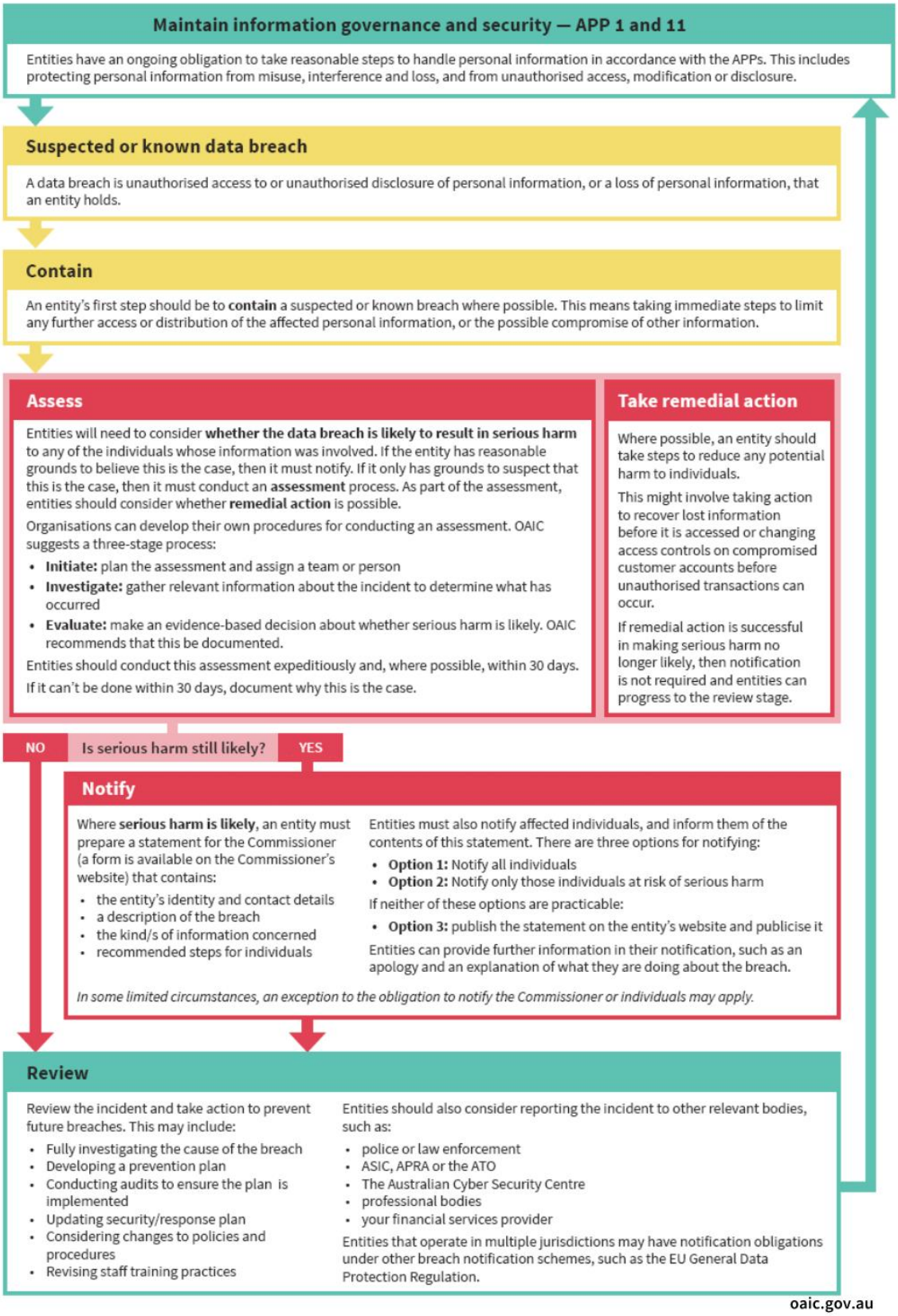
At any time, entities should take remedial action, where possible, to limit the impact of the breach on affected individuals. If remedial action is successful in preventing a likely risk of serious harm to individuals, the NDB scheme notification obligations may not apply.

In general, entities should:

- take each data breach or suspected data breach seriously and move immediately to contain, assess and remediate the incident. Breaches that may initially seem immaterial may be significant when their full implications are assessed
- undertake steps 1 (Contain), 2 (Assess), and 3 (Notify) either simultaneously or in quick succession. In some cases it may be appropriate to notify individuals immediately, before containment or assessment of the breach occurs
- determine how to respond on a case-by-case basis. Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, an entity may take additional steps that are specific to the nature of the breach.

The following diagram summarises the data breach response process. The parts of this process that are required by the NDB scheme are coloured red. The NDB scheme is explained in detail in Part 4 of this guide.

Data breach preparation and response
July 2019



Step 1: Contain

Once an entity has discovered or suspects that a data breach has occurred, it should immediately take action to limit the breach.

For example, stop the unauthorised practice, recover the records, or shut down the system that was breached. If it is not practical to shut down the system, or if it would result in loss of evidence, then revoke or change computer access privileges or address weaknesses in physical or electronic security.

Addressing the following questions may help you identify strategies to contain a data breach:

- How did the data breach occur?
- Is the personal information still being shared, disclosed, or lost without authorisation?
- Who has access to the personal information?
- What can be done to secure the information, or stop the unauthorised access or disclosure, and reduce the risk of harm to affected individuals?

At this point, an entity may suspect an eligible data breach under the NDB scheme has occurred, which would trigger assessment obligations. Or, the entity may believe the data breach is an eligible data breach, which requires them to notify individuals as soon as practicable.

During this preliminary stage, be careful not to destroy evidence that may be valuable in identifying the cause of the breach, or that would enable the entity to address all risks posed to affected individuals or the entity.

Step 2: Assess

An assessment of the data breach can help an entity understand the risks posed by a data breach and how these risks can be addressed. It should be conducted as expeditiously as possible.

Gather and evaluate as much information about the data breach as possible. By creating a complete picture of the data breach, an entity can ensure they understand the risk of harm to affected individuals, and identify and take all appropriate steps to limit the impact of a data breach.

This assessment should also assist entities in deciding whether affected individuals must be notified.

In your assessment of a data breach, consider:

- the type or types of personal information involved in the data breach
- the circumstances of the data breach, including its cause and extent
- the nature of the harm to affected individuals, and if this harm can be removed through remedial action.

All entities should consider whether remedial action can be taken to reduce any potential harm to individuals. This might also take place during Step 1: Contain, such as by recovering lost information before it is accessed.

Entities subject to the NDB scheme are required to conduct an assessment of 'suspected' eligible data breaches and take reasonable steps to complete this assessment within 30 days (see

Assessing a Suspected Data Breach). Criteria for assessing a data breach, including the risk of harm and remedial action, is explored in Identifying Eligible Data Breaches.

Step 3: Notify

Notification can be an important mitigation strategy that has the potential to benefit both the entity and the individuals affected by a data breach. The challenge is to determine when notification is appropriate. Sometimes, notifying individuals can cause undue stress or harm. For example, notifying individuals about a data breach that poses very little or no risk of harm can cause unnecessary anxiety. It can also de-sensitise individuals so that they don't take a notification seriously, even when there is a real risk of serious harm. Each incident needs to be considered on a case-by-case basis to determine whether breach notification is required.

Consider:

- the obligations of the entity under the NDB scheme. Entities are required to notify individuals and the Commissioner about data breaches that are likely to result in serious harm. Part 4 of this guide provides further detail about the NDB scheme's requirements
- other circumstances in which individuals should be notified. For example, your entity may not have obligations under the NDB scheme, but have processes in place to notify affected individuals in certain circumstances
- how notification should occur, including:
  - what information is provided in the notification
  - how the notification will be provided to individuals
  - who is responsible for notifying individuals and creating the notification.
- who else other than affected individuals (and the Commissioner if the notification obligations of the NDB scheme apply) should be notified
- where a law enforcement agency is investigating the breach, it may be appropriate to consult the investigating agency before making details of the breach public
- whether the incident triggers reporting obligations to other entities.

Effective data breach response is about reducing or removing harm to affected individuals, while protecting the interests of your organisation or agency. Notification has the practical benefit of providing individuals with the opportunity to take steps to protect their personal information following a data breach, such as by changing account passwords or being alert to possible scams resulting from the breach. It is important that staff are capable of engaging with individuals who have been affected by a data breach with sensitivity and compassion, in order not to exacerbate or cause further harm. Notification can also help build trust in an entity, by demonstrating that privacy protection is taken seriously.

Step 4: Review

Once steps 1 to 3 have been completed, an entity should review and learn from the data breach incident to improve its personal information handling practices.

This might involve:

- a security review including a root cause analysis of the data breach

- a prevention plan to prevent similar incidents in future
- audits to ensure the prevention plan is implemented
- a review of policies and procedures and changes to reflect the lessons learned from the review
- changes to employee selection and training practices
- a review of service delivery partners that were involved in the breach.

In reviewing information management and data breach response, an entity can refer to the OAIC's Guide to Securing Personal Information.[10]

When reviewing a data breach incident, it is important to use the lessons learned to strengthen the entity's personal information security and handling practices, and to reduce the chance of reoccurrence. A data breach should be considered alongside any similar breaches that have occurred in the past, which could indicate a systemic issue with policies or procedures.

If any updates are made following a review, staff should be trained in any changes to relevant policies and procedures to ensure a quick response to a data breach.

[10] See Guide to Securing Personal Information, OAIC website <https://www.oaic.gov.au>.

Part 4: Notifiable Data Breach (NDB) Scheme

The Privacy Act requires certain entities to notify individuals and the Commissioner about data breaches that are likely to cause serious harm.

The requirements of the NDB scheme are contained in Part IIIC of the Privacy Act and apply to breaches that occur on or after 22 February 2018.

This part of the guide covers the following topics:

- Entities covered by the NDB scheme
- Data breaches involving more than one entity
- Identifying eligible data breaches
- Exceptions to the notification obligation
- Assessing a suspected data breach
- Notifying individuals about an eligible data breach
- What to include in an eligible data breach statement
- The Australian Information Commissioner's role in the NDB scheme.

Entities covered by the NDB scheme

Key points

- Entities that have existing obligations under the Privacy Act to secure personal information must comply with the NDB scheme.
- This includes Australian Government agencies, businesses and not-for profit organisations that have an annual turnover of more than AU$3 million, private sector health service providers, credit reporting bodies, credit providers, entities that trade in personal information and tax file number (TFN) recipients.
- Entities that have Privacy Act security obligations in relation to particular types of information only (for example, small businesses that are required to secure tax file number information) do not need to notify about data breaches that affect other types of information outside the scope of their obligations under the Privacy Act.

APP entities

The NDB scheme applies to entities that have an obligation under APP 11 of the Privacy Act to protect the personal information they hold (s 26WE(1)(a)).[11] Collectively known as 'APP entities', these include Australian Government agencies and private sector and not-for-profit organisations with an annual turnover of more than $3 million. The definition of APP entity generally does not include small business operators, registered political parties, state or territory authorities, or a prescribed instrumentality of a state (s 6C). However, some businesses of any size are APP entities, including businesses that trade in personal information[12] and organisations that provide a health service to, and hold health information about, individuals (see What Is a Health Service Provider?).[13]

For more information about APP entities, see Chapter B of the Australian Privacy Principle Guidelines (APP Guidelines).[14]

Exempt acts and practices, including employee records

The NDB scheme only applies to entities and personal information holdings that are already subject to security requirements under the Privacy Act. This means that acts and practices of APP entities that are exempt from the Privacy Act will also be exempt from the NDB scheme.

For example, in some circumstances, private sector employers do not have to comply with the APPs in relation to employee records associated with current and former employment relationships (s 7B(3)). If an exempt employee record is subject to unauthorised access, disclosure or loss, the private sector employer does not have to assess the breach or notify individuals and the Commissioner. This exemption does not apply to TFN information that is contained within an employee record. However, given community expectations around the handling of their personal

---

[11] 'Personal information' is defined in s 6(1) of the Privacy Act to include information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not.

[12] See Trading in Personal Information, OAIC website <https://www.oaic.gov.au>.

[13] See What Is a Health Service Provider?, OAIC website <https://www.oaic.gov.au>.

[14] See APP Guidelines, Chapter B: Key Concepts, section 'APP entity', OAIC website <https://www.oaic.gov.au>.

information, it is recommended that employers notify affected individuals where a breach of an employee record is likely to result in serious harm. Doing so will enable affected individuals to take protective action against any potential harms, as well as illustrating to employees that the security of their records is taken seriously.

Further information about acts and practices that are exempt from the APPs and, by extension, the NDB scheme can be found in Rights and Responsibilities.[15]

Small business operators

A small business operator (SBO) is an individual (including a sole trader), body corporate, partnership, unincorporated association, or trust that has not had an annual turnover of more than $3 million in any financial year since 2001 (s 6D).

Generally, SBOs do not have obligations under the APPs unless an exception applies (s 6D(4)).

In certain circumstances an SBO must comply with the APPs, and therefore with the NDB scheme. That will be the case where the SBO

- holds health information and provides a health service
- is related to an APP entity
- trades in personal information. That is, the SBO discloses personal information about individuals to anyone else for a benefit, service or advantage; or provides a benefit, service or advantage through the collection of personal information about another individual from anyone else
- is a credit reporting bodies
- is an employee associations registered under the Fair Work (Registered Organisations) Act 2009
- has 'opted-in' to APP coverage under s 6EA of the Privacy Act.

If an SBO carries on certain activities it must comply with the APPs, and therefore must comply with the NDB scheme, but only in relation to personal information held by the entity for the purpose of, or in connection with, those activities. Those activities include:

- providing services to the Commonwealth under a contract
- operating a residential tenancy data base
- reporting under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006
- conducting a protected action ballot
- information retained under the mandatory data retention scheme, as per Part 5-1A of the Telecommunications (Interception and Access) Act 1979.

More information about how to determine whether a business or organisation is an APP entity or subject to the APPs for some of its activities is available at Small Business.[16]

[15] See Rights and Responsibilities, OAIC website <https://www.oaic.gov.au>.

[16] See Small Business, OAIC website <https://www.oaic.gov.au>.

Credit reporting bodies

A credit reporting body (CRB) is a business or undertaking that involves collecting, holding, using, or disclosing personal information about individuals for the purpose of providing an entity with information about the credit worthiness of an individual (s 6P). Credit reporting information is defined as credit information or CRB derived information about an individual (s 6(1)).

CRBs have obligations under the NDB scheme in relation to their handling of credit reporting information (s 26WE(1)(b)), and in relation to their handling of any other personal information for which they have obligations under APP 11.

Credit providers

The NDB scheme applies to all credit providers whether or not they are APP entities. The section of the Privacy Act under which a credit provider is required to comply with the scheme will depend on what kind of information is involved in the data breach.

If it is 'credit eligibility information' (defined in s 6(1)) the NDB scheme will apply because of the security requirement in s 21S(1) in relation to that information.

If the credit provider is also an APP entity the NDB scheme applies in relation to other personal information because of the security requirement in APP 11.

The organisations that are credit providers for the purposes of the Privacy Act (s 6G) are:

- a bank
- an organisation or small business operator if a substantial part of its business is the provision of credit, such as a building society, finance company or a credit union
- a retailer that issues credit cards in connection with the sale of goods or services
- an organisation or SBO that supplies goods and services where payment is deferred for seven days or more, such as telecommunications carriers, and energy and water utilities
- certain organisations or SBOs that provide credit in connection with the hiring, leasing, or renting of goods.

An organisation or SBO that acquires the right of a credit provider in relation to the repayment of an amount of credit is also considered a credit provider, but only in relation to that particular credit (s 6K).

TFN recipients

The NDB scheme applies to TFN recipients[17] in relation to their handling of TFN information (s 26WE(1)(d)). A TFN recipient is any person who is in possession or control of a record that contains TFN information (s 11). TFN information is information that connects a TFN with the identity of a particular individual (s 6).

A TFN recipient may also be an APP entity or credit provider. In certain circumstances, entities that are not otherwise covered by the Privacy Act, such as state and local government bodies, may also be authorised to receive TFN information and will be considered TFN recipients.

[17] Referred to in the Privacy Act and Privacy (Tax File Number) Rule 2015 as 'file number recipients'.

The NDB scheme applies to TFN recipients to the extent that TFN information is involved in a data breach. If TFN information is not involved, a TFN recipient would only need to comply with the NDB scheme for breaches of other types of information if they are also a credit provider or APP entity.

More information about TFN recipients is available in The Privacy (Tax File Number) Rule 2015 and the Protection of Tax File Number Information.[18]

Overseas activities

Entities with an 'Australian link'

The NDB scheme generally extends to the overseas activities of an Australian Government agency (s 5B(1)). It also applies to organisations (including small businesses covered by the Act, outlined above) that have an 'Australian link' (s 5B(2)).

An organisation has an Australian link either because it is, in summary, incorporated or formed in Australia (see s 5B(1A) for more detail), or where:

- it carries on business in Australia or an external Territory, and
- it collected or held personal information in Australia or an external Australian Territory, either before or at the time of the act or practice (s 5B(3)).

Further information about entities that are taken to have an Australian link is available in Chapter B of the APP Guidelines.[19]

Disclosing personal information overseas

If an APP entity discloses personal information to an overseas recipient, in line with the requirements of APP 8.1, then the APP entity is deemed to 'hold' the information for the purposes of the NDB scheme (s 26WC(1)). APP 8.1 says that an APP entity that discloses personal information to an overseas recipient is required to take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information. This means that if the personal information held by the overseas recipient is subject to loss, unauthorised access, or disclosure, the APP entity is still responsible for assessing whether it is an eligible data breach under the Privacy Act, and if it is, for notifying individuals at risk of serious harm and providing a statement to the Commissioner.

There are exceptions to the requirement in APP 8.1 to take reasonable steps. APP entities that disclose information overseas under an exception in APP 8.2 are not taken to 'hold' information they have disclosed overseas under s 26WC. In these circumstances, if the personal information held by the overseas recipient is subject to a data breach, the APP entity does not have obligations to notify about the breach under the NDB scheme.

More information about APP 8 is available in Sending Personal Information Overseas.[20]

---

[18] See The Privacy (Tax File Number) Rule 2015 and the Protection of Tax File Number Information, OAIC website <https://www.oaic.gov.au>.

[19] See APP Guidelines, Chapter B: Key Concepts, section 'Australian link', OAIC website <https://www.oaic.gov.au>.

[20] See Sending Personal Information Overseas, OAIC website <https://www.oaic.gov.au>.

Disclosing credit eligibility information

If a credit provider discloses credit eligibility information about one or more individuals to a person, a body or a related body corporate that does not have an 'Australian link' (s 26WC(2)(a)),[21] the credit provider may also have obligations under the NDB scheme in respect of that information. In the event that credit eligibility information held by the person or related body corporate is subject to loss, unauthorised access, or disclosure, the credit provider is responsible for assessing whether there is an eligible data breach that needs to be notified to individuals at risk of serious harm and the Commissioner.

[21] This section only applies to a disclosure of credit eligibility information by a credit provider to a related body corporate under s 21G(3)(b), to a person processing an application for credit made to the credit provider or to a person who manages credit provided by the credit provider under s 21G(3) or to a debt collector under s 21M(1) of the Privacy Act.

Data breaches involving more than one entity

Key points

- The NDB scheme recognises that entities often hold personal information jointly. For example, one entity may have physical possession of the information, while another has legal control or ownership.
- In these circumstances, an eligible data breach of one entity will also be considered an eligible data breach of other entities that hold the affected information. Both will have obligations under the NDB scheme.
- In general, compliance by one entity will also be taken as compliance by each of the entities that hold the information. As such, only one entity needs to take the steps required by the NDB scheme. The NDB scheme leaves it up to the entities to decide which of them should do so.
- OAIC suggests that, in general, the entity with the most direct relationship with the individuals affected by the data breach should carry out notification.

When is information held jointly?

Under s 6(1) of the Privacy Act, an entity is taken to 'hold' personal information if it has possession or control of a record that contains personal information. This means that the term 'holds' extends beyond physical possession of a record to include a record that an entity has a right or power to deal with, even if it does not physically possess the record or own the medium on which it is stored.

For example, one entity may store its records with a cloud service provider. Since the cloud service provider has possession of the records, it will be taken to hold the personal information. Because the first entity has contractual rights to retain control of the records (such as maintaining rights to access and use the records), both entities hold the information.

Whether an entity will be taken to 'hold' personal information will therefore depend on the particular circumstances of the arrangement.

Other examples where two or more entities may hold the same information include:

- outsourcing arrangements
- Commonwealth contracts
- joint ventures.

Example
A large market research company is conducting focus groups on behalf of its client, a fast food outlet, using a list of interviewees provided by its client for that purpose. The contractual arrangements between the market research company and the fast food outlet give the fast food outlet effective control over how the information is handled by the research company. Following the focus group sessions, all participants give consent to participate in future research projects for the research company's other clients. The research company creates a new record containing the participant's names and contact details. Although the record contains the same information that the market research company originally received from the fast food outlet, only the market research company has possession or control over the newly created record. This means that only the market research company would have NDB scheme obligations in the event of a data breach affecting the newly created record.

Responding to data breaches of jointly held information

In situations where two or more entities hold the same record of personal information, both entities are generally responsible for complying with the NDB scheme in relation to this record.

However, exceptions apply so that only one of the entities that jointly holds information needs to comply with the NDB scheme's assessment and notification requirements on behalf of the group. For example, if a data breach affects one or more other entities that jointly hold personal information, and one entity has assessed the suspected breach, the other entities are not required to also assess the breach (s 26WJ). If no assessment is conducted, depending on the circumstances, each entity that holds the information may be found to be in breach of the assessment requirements.

Similarly, only one entity needs to notify individuals and the Commissioner (s 26WM) if there is an eligible data breach involving personal information jointly held by more than one entity (see Identifying Eligible Data Breaches). If none of the entities notify, then all of the entities may be found to have breached the notification requirements of the NDB scheme (s 26WL(2)).

See Exceptions to Notification Obligations for more information about the circumstances in which specific exceptions apply to entities that jointly hold information.

How to allocate responsibility for compliance

Each entity that holds personal information involved in an eligible data breach, should be able to demonstrate they are meeting the requirements of the NDB scheme.

The NDB scheme does not prescribe which entity should conduct an assessment of a suspected data breach, nor which entity should notify individuals and the Commissioner about an eligible data breach. This allows entities to tailor their arrangements to accommodate their particular contractual and customer relationships.

Accordingly, where information is held jointly, entities should establish clear procedures for complying with the NDB scheme when entering into service agreements or other relevant contractual arrangements. This may include considering obligations around the communication of suspected breaches, processes for conducting assessments, and responsibility for containment, remediation, and notification.

The Commissioner suggests that, in general, the entity with the most direct relationship with the individuals at risk of serious harm may be best placed to notify. This will allow individuals to better understand the notification, and how the eligible data breach might affect them.

Example

A medical practice stores paper-based patient records with a contracted storage provider. The storage provider's premises are broken into and a number of items stolen. While the storage provider cannot immediately determine if the stolen items included the medical practice's records, it suspects that they might have been included. Both the medical practice and the storage provider hold the records for the purpose of the Privacy Act, so both have an obligation to conduct an assessment and, if required, notify.

Since the storage provider is more familiar with its facilities, the entities decide that the storage provider is best placed to conduct an assessment and determine if the records were stolen. Once the provider determines that the records were stolen, the medical practice assists the assessment by using its knowledge about the affected individuals to conclude that serious harm is likely. Although the storage provider's insurance company has agreed to cover the cost of notification, the storage provider and medical practice agree that it is most appropriate that notification come from the medical practice, as the relevant individuals do not have any pre-existing relationship with the storage provider. As such, the medical practice notifies the individuals about the incident and is reimbursed by the storage provider and its insurer for the costs of notification.

Identifying eligible data breaches

Key points

- The NDB scheme requires regulated entities to notify particular individuals and the Commissioner about 'eligible data breaches'. A data breach is eligible if it is likely to result in serious harm to any of the individuals to whom the information relates.
- Whether a data breach is likely to result in serious harm requires an objective assessment, determined from the viewpoint of a reasonable person in the entity's position.
- Not all data breaches are eligible. For example, if an entity acts quickly to remediate a data breach, and as a result of this action the data breach is not likely to result in serious harm, there is no requirement to notify any individuals or the Commissioner. There are also exceptions to notifying in certain circumstances.

Eligible data breach

An eligible data breach arises when the following three criteria are satisfied:

1. there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds (see, What is a 'Data Breach'?)
2. this is likely to result in serious harm to one or more individuals (see, Is Serious Harm Likely?), and
3. the entity has not been able to prevent the likely risk of serious harm with remedial action (see Preventing Serious Harm With Remedial Action).

This document is about the threshold at which an incident is considered an 'eligible data breach' that will be notifiable under the scheme unless an exception applies. Assessing a Suspected Data Breach provides guidance to entities about the process to follow when carrying out an assessment of 'whether there are reasonable grounds to suspect that there may have been an eligible data breach of the entity' under s 26WH.

What is a 'data breach'?

The first step in deciding whether an eligible data breach has occurred involves considering whether there has been a data breach; that is, unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information (s 26WE(2)). The Privacy Act does not define these terms. The following analysis and examples draw on the ordinary meaning of these words.

- ***Unauthorised access*** of personal information occurs when personal information that an entity holds is accessed by someone who is not permitted to have access. This includes unauthorised access by an employee of the entity, or an independent contractor, as well as unauthorised access by an external third party (such as by hacking).

  Examples of unauthorised access include:

  - an employee browsing sensitive customer records without any legitimate purpose
  - a computer network being compromised by an external attacker resulting in personal information being accessed without authority.

- ***Unauthorised disclosure*** occurs when an entity, whether intentionally or unintentionally, makes personal information accessible or visible to others outside the entity and releases that information from its effective control in a way that is not permitted by the Privacy Act. This includes an unauthorised disclosure by an employee of the entity.

  For example, an employee of an entity accidentally publishing a confidential data file containing the personal information of one or more individuals on the internet would be considered unauthorised disclosure

- ***Loss*** refers to the accidental or inadvertent loss of personal information held by an entity, in circumstances where is it is likely to result in unauthorised access or disclosure.

  An example is where an employee of an entity leaves personal information (including hard copy documents, unsecured computer equipment, or portable storage devices containing personal information) on public transport. Under the NDB scheme, if personal information is lost in circumstances where subsequent unauthorised access to or disclosure of the information is unlikely, there is no eligible data breach (s 26WE(2)(b)(ii)). For example, if the personal information is remotely deleted before an unauthorised person could access the information, or if the information is encrypted to a high standard making unauthorised access or disclosure unlikely, then there is no eligible data breach.

Is serious harm likely?

The second step in deciding whether an eligible data breach has occurred involves deciding whether, from the perspective of a reasonable person, the data breach would be likely to result in serious harm to an individual whose personal information was part of the data breach.

For the NDB scheme a 'reasonable person' means a person in the entity's position (rather than the position of an individual whose personal information was part of the data breach or any other person), who is properly informed, based on information immediately available or following reasonable inquiries or an assessment of the data breach. In general, entities are not expected to make external enquiries about the circumstances of each individual whose information is involved in the breach. 'Reasonable person' is also discussed in general terms in Chapter B of the OAIC's APP Guidelines.[22]

The phrase 'likely to occur' means the risk of serious harm to an individual is more probable than not (rather than possible).

'Serious harm' is not defined in the Privacy Act. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm.

Entities should assess the risk of serious harm holistically, having regard to the likelihood of the harm eventuating for individuals whose personal information was part of the data breach and the consequences of the harm. The NDB scheme includes a non-exhaustive list of 'relevant matters' that may assist entities to assess the likelihood of serious harm. These are set out in s 26WG as follows:

- the kind or kinds of information

[22] See APP Guidelines, Chapter B: Key Concepts, section 'Reasonable, reasonably', OAIC website <https://www.oaic.gov.au>. .

- the sensitivity of the information
- whether the information is protected by one or more security measures
- if the information is protected by one or more security measures – the likelihood that any of those security measures could be overcome
- the persons, or the kinds of persons, who have obtained, or who could obtain, the information
- if a security technology or methodology:
  - was used in relation to the information, and;
  - was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information
- the likelihood that the persons, or the kinds of persons, who:
  - have obtained, or who could obtain, the information, and;
  - have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates;
  - have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology
- the nature of the harm
- any other relevant matters.

As some of these matters involve overlapping considerations, they are discussed further below, under the broader headings:

1. the type or types of personal information involved in the data breach
2. the circumstances of the data breach
3. the nature of the harm that may result from the data breach.

The type or types of personal information involved in the data breach

Some kinds of personal information may be more likely to cause an individual serious harm if compromised. Examples of the kinds of information that may increase the risk of serious harm if there is a data breach include:

- 'sensitive information',[23] such as information about an individual's health
- documents commonly used for identity fraud (including Medicare card, driver licence, and passport details)
- financial information
- a combination of types of personal information (rather than a single piece of personal information) that allows more to be known about the individuals the information is about.

[23] See s 6(1) of the Privacy Act for categories of personal information that are covered by the definition of 'sensitive information'.

Circumstances of the data breach

The specific circumstances of the data breach are relevant when assessing whether there is a risk of serious harm to an individual. This may include consideration of the following:

- **Whose personal information was involved in the breach?** An entity could consider whose personal information was involved in the breach, as certain people may be at particular risk of serious harm. A data breach involving the names and addresses of individuals might not, in various circumstances, be likely to result in serious harm to an individual, particularly if that information is already publicly available. However, if the entity knows that the information involved primarily relates to individuals known to be vulnerable, this may increase the risk of serious harm
- **How many individuals were involved?** If the breach involves the personal information of many individuals, the scale of the breach should affect an entity's assessment of likely risks. Even if an entity considers that each individual will only have a small chance of suffering serious harm, if more people's personal information is involved in the breach, it may be more likely that at least some of the individuals will experience serious harm. From a risk perspective, it may be prudent, depending on the particular circumstances, to assume a breach involving the personal information of a very large number of people is likely to result in serious harm to at least one of those individuals, unless context or circumstances would support this not being the case
- **Do the circumstances of the data breach affect the sensitivity of the personal information?** A breach that may publicly associate an individual's personal information with a sensitive product or service they have used may increase the risk of serious harm. For example, a data breach involving an individual's name may involve a risk of serious harm if the entity's name links the individual with a particular form of physical or mental health care[24]
- **How long has the information been accessible?** The time between when the data breach occurred and when the entity discovers the breach will be relevant to the entity's consideration of whether serious harm is likely to occur. For example, if personal information is publically accessible for a significant period before the entity is aware of the data breach, it may be more likely that the personal information have been accessed in ways that will result in serious harm to the individuals affected
- **Is the personal information adequately encrypted, anonymised, or otherwise not easily accessible?** A relevant consideration is whether the information is rendered unreadable through the use of security measures to protect the stored information, or if it is stored in such a way so that it cannot be used if breached. In considering whether security measures (such as encryption) applied to compromised data are adequate, the entity should consider whether the method of encryption is an industry-recognised secure standard at the time the entity is assessing the likelihood of risk. Additionally, an entity should have regard to whether the unauthorised recipients of the personal information would have the capability to circumvent these safeguards. For example, if an attacker holds both encrypted data and the encryption key needed to decrypt that data, the entity should not assume the data is secure
- **What parties have gained or may gain unauthorised access to the personal information?** The unauthorised disclosure of an individual's criminal record to someone who knows that

[24] Another example would include the information disclosed in the Ashely Madison data breach in 2015. See Ashley Madison Joint Investigation, OAIC website <https://www.oaic.gov.au>.

individual personally may increase the risk of serious reputational harm for that individual. In addition, where a third party that obtains unauthorised access to personal information, or appears to target personal information of a particular individual or group of individuals, this may increase the risk of serious harm as it may be more likely the personal information is intended for malicious purposes.

The nature of the harm

In assessing the risk of serious harm, entities should consider the broad range of potential kinds of harms that may follow a data breach. It may be helpful for entities assessing the likelihood of harm to consider a number of scenarios that would result in serious harm and the likelihood of each. Examples may include:

- identity theft
- significant financial loss by the individual
- threats to an individual's physical safety
- loss of business or employment opportunities
- humiliation, damage to reputation or relationships
- workplace or social bullying or marginalisation.

The likelihood of a particular harm occurring, as well as the anticipated consequences for individuals whose personal information is involved in the data breach if the harm materialises, are relevant considerations.

Preventing serious harm with remedial action

The NDB scheme provides entities with the opportunity to take positive steps to address a data breach in a timely manner, and avoid the need to notify. If an entity takes remedial action such that the data breach would not be likely to result in serious harm, then the breach is not an eligible data breach for that entity or for any other entity (s 26WF(1), s 26WF(2), s 26WF(3)). For breaches where information is lost, the remedial action is adequate if it prevents unauthorised access to, or disclosure of personal information (s 26WF(3)).

If the remedial action prevents the likelihood of serious harm to some individuals within a larger group of individuals whose information was compromised in a data breach, notification to those individuals for whom harm has been prevented is not required.

Examples of remedial action that may prevent serious harm occurring include:

Example 1

A data file, which includes the personal information of numerous individuals, is sent to an incorrect recipient outside the entity. The sender realises the error and contacts the recipient, who advises that the data file has not been accessed. The recipient has an ongoing contractual relationship with the sender, and regards the recipient as reliable and trustworthy. The sender then confirms that the recipient has not copied, and has permanently deleted the data file. In the circumstances, the sender decides that there is no likely risk of serious harm.

Example 2

An employee leaves a smartphone on public transport while on their way to work. When the employee arrives at work they realise that the smartphone has been lost, and ask their employer's IT support staff to remotely delete the information on the smartphone. Because of the security measures on the smartphone, the IT support staff are confident that its content could not have been accessed in the short period between when it was lost and when its contents were deleted.

Examples of data breaches

The following examples are provided to illustrate some of the considerations that entities might take into account when assessing whether a data breach is likely to result in serious harm. However, whether any data breach is notifiable depends on the particular circumstances of the breach.

The acts and practices described in these examples may raise other issues under the Privacy Act, such as whether these organisations have taken reasonable steps to secure personal information, as required by APP 11.1.

Example 1 — strong encryption making notification unnecessary

Insure, an insurance company, decides to update its customer relationship management and record keeping software. While running a test, the IT team installing the software discovers that some customer records were accessed by an unauthorised third party more than a year ago. The customer records involved are primarily encrypted payment card information.

Since Insure suspects fraudulent activity as the motive for the unauthorised access, it notifies the police and hires an external IT security consultant to conduct an audit and security assessment. The audit confirms that 500 customer records were involved in the data breach, and that an overseas source was responsible for the hack. The IT security consultant's comprehensive sweeps of the internet and dark web were unable to find evidence that the information was offered for sale or otherwise disclosed online. The IT security consultant also assesses that because of the high standard of encryption used for the credit card information, it is unlikely that this information could be accessed by the hacker. Insure implemented the recommendations of its IT security consultant, including new IT security protocols and intrusion detection software.

Insure determines that it is not likely that the individuals whose personal information is involved in the data breach are at risk of serious harm. Therefore, Insure decides it is not an eligible data breach, and is not required to notify affected individuals or the Commissioner.

Nonetheless, it decides that as a customer service measure, it should tell the individuals about the incident. It sends an email to the customers informing them of the incident and providing some advice on personal information security measures they can take. This notification is not required by the NDB scheme, so can take any form that Insure considers appropriate.

Example 2 — notification following unintentional publication of sensitive data

Medicines, a chain of low-cost pharmacies, becomes aware that its customer database, including records about dispensing of prescription drugs, has been publicly available on the internet due to a technical error. Medicines' security consultants identify that the database was publicly available for a limited time and that it was only accessed a few times.

However, Medicines is unable to determine who accessed the data or if they kept a copy. Given the sensitivity of the personal information contained in the database, including drugs related to the treatment of addictive and psychiatric conditions, Medicines' risk assessment concludes that the data breach would be likely to result in serious harm to some of its customers.

Medicines decides to notify all customers whose personal information is involved in the data breach and the Commissioner. Because it does not have contact details for many of the customers who filled prescriptions with it in person, it publishes a notice describing the breach on its website and posts a copy in a prominent location at each of its stores.

Example 3 — data breach experienced by overseas contractor leading to phishing

Consumestuff enters into a contract with an automated email marketing platform located overseas, which it uses to communicate with its customers. The service provider detects that the bulk mailing distribution lists for Consumestuff have been downloaded by an external IP address. The bulk mailing distribution lists include the name, email address, gender, and suburb of Consumestuffs' customers. The service provider notifies Consumestuff, who conducts an immediate investigation into how the mailing lists were accessed and downloaded.

An IT security sweep detects malware on a Consumestuff employee's computer, and the investigation concludes that the employee's login credentials for the service provider were obtained after the employee unintentionally opened an email attachment from a malicious third party attacker. As Consumestuff also held the personal information, and assuming that the service provider is not an APP entity, Consumestuff undertakes an assessment to determine whether it is required to notify individuals and the Commissioner.

As part of its assessment, Consumestuff identifies that some of the individuals whose personal information was involved in the data breach received emails that fraudulently claimed to be sent from Consumestuff asking for customer credit card details. Given this information, Consumestuff concludes that it is more probable than not that the attacker will use the information in the mailing lists for the purposes of fraud or identity theft, and that it is likely that some of the individuals will suffer serious financial harm as a result of this.

Given this likelihood, Consumestuff sends an email with the relevant information required by the NDB scheme to those individuals whose personal information is involved in the data breach, and notifies the Commissioner. Consumestuffs' email to these individuals includes information about scam emails and how to identify them, and provides referrals to services that assist individuals in mitigating the risk of identity theft.

Example 4 — loss of unencrypted storage media containing personal information

A member of the human resources team of a Government Department (the Department) copies the employee records of the Department's 2000 employees onto a portable memory stick, to do work at home. This action was in breach of the Department's policies, and Australian Privacy Principle 11. The memory stick is lost by the employee who held it. They report this to their manager.

The Department follows its data breach response plan, and as a first step conducts a search for the memory stick, but fails to locate it. The information contained in the memory stick includes the names, salary information, TFNs, home addresses, phone numbers, birth dates, and in some cases health information (including disability information) of current staff. As the data on the memory stick is not encrypted, the Department concludes that unauthorised access is likely to occur.

Due to the sensitivity of the unencrypted information – not only the extent and variety of the information, but also the inclusion of health and disability information in the records – the Department's risk assessment finds that there is a likely risk of serious harm to at least one of the individuals whose personal information is involved in the data breach. On this basis, the Department considers that it is an eligible data breach for the purposes of the NDB scheme, and prepares a statement to notify the Commissioner.

A senior staff member emails the relevant staff to notify them of the eligible data breach, and provides the content of the statement prepared for the Commissioner. In the notification, the Department also offers staff an apology for the breach, notes that the OAIC has been informed of the breach, and explains what steps have been put in place to prevent this type of a breach occurring in the future.

Example 5 — online banking fraud and remedial action

A bank's fraud detection systems flag that there has been unusual activity on an individual's online banking account, when a substantial amount of money is transferred to an account in another country. The fraud team assesses the activity, and finds that the account was accessed by an unauthorised attacker who had obtained control of the individual's account.

Through its existing fraud management processes, the bank's fraud team notify the individual that it is temporarily freezing online access to the account due to the fraudulent activity, resets the password for online access and returns the stolen funds. As part of its risk assessment, the fraud team confirms that the individual's other accounts have not been compromised, and recommends to the individual that they change any similar passwords to other services. A member of the bank's fraud team assesses whether there is a risk of likely harm to the individual, and concludes that as a result of the above steps taken to remediate the unauthorised access, it is not likely the individual will be at risk of serious harm. Given this remedial action, the bank does not notify the Commissioner.

Example 6 — email sent to the wrong recipient contained before serious harm can occur

CareHeeps, a claims management service provider, regularly sends updates to its clients about the status of the workers compensation claims of their employees. Because of human error, an employee of CareHeeps accidentally sends an email with an attachment about the employees of Business A to another client, Business B. The attachment contains the personal information of 200 employees of Business A, and includes their name, address, date of birth, and health information about their claimed injury.

A CareHeeps employee realises the error, and contacts Business B to delete the email with the attachment. Business B confirms that one of its employees accessed the file without initially realising the error, but provides written confirmation that it has since deleted all copies of the email and attachment. The employee who accessed the file has also undertaken not to divulge the information. CareHeeps' assessment of the remedial action taken concludes that, while the file included sensitive information about the individuals' health, its contractual arrangements with Business B and the written assurance provided by Business B has prevented the likely risk of serious harm to any individuals. As a consequence, CareHeeps determines that it is not an eligible data breach that needs to be notified to individuals or the Commissioner.

Exceptions to notification obligations

Key points

- The NDB scheme requires regulated entities to notify individuals and the Commissioner of 'eligible data breaches'. A data breach is an eligible data breach if an individual is likely to experience serious harm (see Identifying Eligible Data Breaches and Notifying Individuals About an Eligible Data Breach).
- There are some exceptions to the notification requirements, which relate to:
  - eligible data breaches of other entities (see Data Breaches Involving More Than One Entity)
  - enforcement related activities
  - inconsistency with secrecy provisions
  - declarations by the Commissioner.
- Data breaches that are notified under s 75 of the My Health Records Act, do not need to be notified under the NDB scheme.

Enforcement related activities

An enforcement body does not need to notify individuals about an eligible data breach if its chief executive officer (CEO) believes on reasonable grounds that notifying individuals would be likely to prejudice an enforcement related activity conducted by, or on behalf, of the enforcement body (s 26WN).[25]

'Believes on reasonable grounds' means the CEO must have a basis for the belief. It is the responsibility of the enforcement body to be able to justify the reasonable grounds for this belief, and the decision should be documented. 'Reasonable belief' is discussed further in Chapter B of the OAIC's APP Guidelines.[26]

The enforcement body must still provide a statement about the eligible data breach to the Commissioner (see What to Include in an Eligible Data Breach Statement). However, this statement does not have to include the steps recommended for individuals to take in response to the data breach, because individuals are not being notified (s 26WN).

If this exception applies, and the eligible data breach involves other entities, these other entities are not required to notify individuals (s 26WN(e)). Further, these other entities are not required to provide a statement about the eligible data breach to the Commissioner if the enforcement body has done so (s 26WM). To rely on this exception, other entities would usually need a written statement regarding the eligible data breach, dated and signed by the CEO of the enforcement body.

This exception does not apply if an eligible data breach is unrelated to an enforcement activity. For example, the exception may not apply to an eligible data breach involving employees' personal information, which is unrelated to an investigation.

---

[25] See s 6(1) of the Privacy Act for definitions of enforcement body and enforcement related activity.

[26] Paragraphs B.110-B.111.

Inconsistency with secrecy provisions

Exceptions to notifying individuals or the Commissioner may apply where a Commonwealth law prohibits or regulates the use or disclosure of information (a secrecy provision). In particular:

- the requirement to provide a statement to the Commissioner about the eligible data breach does not apply to the extent that this requirement is inconsistent with a secrecy provision (s 26WP(2))
- the requirement to notify individuals about an eligible data breach does not apply to the extent that providing this notice is inconsistent with a secrecy provision (s 26WP(3)).

The exceptions in s 26WP are intended to preserve the operation of specific secrecy provisions in other legislation. A common purpose of secrecy provisions is to prohibit the unauthorised disclosure of client information. Most secrecy provisions allow the disclosure of information in certain circumstances, such as with an individual's consent where the information relates to them, or where the disclosure of information relates to an officer's duties, or the exercise of their powers or functions.

If an eligible data breach occurs, agencies should apply the exceptions under s 26WP only to the extent necessary to avoid inconsistency with a secrecy provision.

For example, if providing a statement about an eligible data breach to the Commissioner (s 26WK) would not be inconsistent with a secrecy provision, but notifying individuals (s 26WL) would be, the entity would only be required to notify the Commissioner.

The following is relevant in assessing whether a secrecy provision is inconsistent with the requirements of the NDB scheme:

- If a secrecy provision permits the disclosure of information that is required or authorised by another law (such as the Privacy Act), there would not be an inconsistency between the secrecy provision and the NDB scheme notification requirements.
- If a secrecy provision does not allow the disclosure of information, even if the disclosure is required or authorised by another law (such as the Privacy Act), there may be inconsistency between the secrecy provision and the NDB scheme notification requirements.
- If a secrecy provision permits the disclosure of information in the course of an officer's duties, there would not be inconsistency between the secrecy provision and the NDB scheme notification requirements, as complying with the notification requirements is the responsibility of the agency through its officers.

Declarations by the Australian Information Commissioner

In some circumstances, the Commissioner may declare by written notice that an entity does not need to comply with the NDB scheme notification requirements (s 26WQ) in relation to a specific eligible data breach. The purpose of the declaration by the Commissioner is to provide an exception where compliance with the NDB notification requirements would conflict with the public interest.

The Commissioner may declare that an entity is not required to provide a statement to the Commissioner or to notify particular individuals (s 26WQ(1)(c)), or that notification to individuals is delayed for a specified period (s 26WQ(1)(d)).

The Commissioner cannot make a declaration under s 26WQ unless satisfied that it is reasonable in the circumstances to do so, having regard to the public interest, relevant advice received from an enforcement body or the Australian Signals Directorate, and any other relevant matter. While the Commissioner is empowered to make a declaration if it is 'reasonable in the circumstances to do so', the Commissioner still has discretion about whether to make a declaration, and on what terms.

In deciding whether to make a declaration, and on what terms, the Commissioner will have regard to the Objects of the Privacy Act and other relevant matters. The Commissioner will consider whether the risks associated with notifying of a particular eligible data breach outweigh the benefits of notification to individuals at risk of serious harm.

Given the clear objective of the scheme to promote notification of eligible data breaches, and the inclusion of exceptions in the scheme that remove the need to notify in a wide range of circumstances, the Commissioner expects that declarations under s 26WQ will only be made in exceptional cases and only after a compelling case has been put forward by the entity seeking the declaration.

The procedure for applying for a declaration, and factors the Commissioner may consider, are outlined in the OAIC's Guide to Privacy Regulatory Action — Chapter 9: Data Breach Incidents.

My Health Record system data breaches

Certain participants in the My Health Record system (such as the System Operator, a registered healthcare provider organisation, a registered repository operator, a registered portal operator or a registered contracted service provider), are required to report data breaches that occur in relation to the My Health Record system to the either the System Operator or the Commissioner, or both, depending on the entity reporting the data breach (s 75 of the My Health Records Act). If a data breach has been, or is required to be, notified under s 75 of the My Health Records Act, the NDB scheme does not apply (s 26WD). This exception is intended to avoid duplication of notices under the NDB scheme and the data breach notification requirements in the My Health Record system.

Information about data breach notification requirements of the My Health Records Act is available in the OAIC's Guide to Mandatory Data Breach Notification in the My Health Record System.[27]

Only notifications under s 75 of the My Health Records Act fall within this exception. Notifications under other schemes such as that within the National Cancer Screening Register Act are not excluded from the NDB scheme.

[27] See Guide to Mandatory Data Breach Notification in the My Health Record System, OAIC website <https://www.oaic.gov.au>.

Example

A practice manager who has access to the My Health Record system for administrative purposes only, accesses a patient's My Health Record clinical information without authorisation. The GP discovers this incident and immediately notifies the System Operator and the Commissioner as required under s 75 of the My Health Records Act. There is no need to also notify this data breach under the Privacy Act.

At or about the same time, the practice manager also accesses the GP's clinical database (not part of the My Health Record system), and downloads their ex-partner's health information without authorisation. Upon discovering this incident, the GP takes immediate steps to contain the breach and, due to the nature of the relationship between the practice manager and the patient, decides there is a likelihood of serious harm to the patient in the circumstances. The GP notifies the patient and the Commissioner about the data breach, as required under the Privacy Act's NDB scheme.

Assessing a suspected data breach

Key points

- If an entity has reasonable grounds to *believe that it has* experienced an eligible data breach, it must promptly notify individuals and the Commissioner about the breach, unless an exception applies.
- In contrast, if an entity *suspects that it may* have experienced an eligible data breach, it must quickly assess the situation to decide whether or not there has been an eligible data breach.
- An assessment must be reasonable and expeditious, and entities may develop their own procedures for assessing a suspected data breach.

When must entities assess a suspected breach?

The NDB scheme is designed so that only serious ('eligible') data breaches are notified (see Identifying Eligible Data Breaches). If an entity is aware of reasonable grounds to *believe that there has been* an eligible data breach, it must promptly notify individuals at risk of serious harm and the Commissioner about the eligible data breach (see Notifying Individuals About an Eligible Data Breach).

On the other hand, if an entity only has reason to *suspect that there may have been* a serious breach, it needs to move quickly to resolve that suspicion by assessing whether an eligible data breach has occurred. If, during the course of an assessment, it becomes clear that there has been an eligible breach, then the entity needs to promptly comply with the notification requirements.

The requirement for an assessment is triggered if an entity is aware that there are reasonable grounds to suspect that there may have been a serious breach (s 26WH(1)).

Whether an entity is 'aware' of a suspected breach is a factual matter in each case, having regard to how a reasonable person who is properly informed would be expected to act in the circumstances. For instance, if a person responsible for compliance or personnel with appropriate seniority are aware of information that suggests a suspected breach may have occurred, an assessment should be done. An entity should not unreasonably delay an assessment of a suspected eligible breach, for instance by waiting until its CEO or board is aware of information that would otherwise trigger reasonable suspicion of a breach within the entity.

The Commissioner expects entities to have practices, procedures, and systems in place to comply with their information security obligations under APP 11, enabling suspected breaches to be promptly identified, reported to relevant personnel, and assessed if necessary.

How quickly must an assessment be done?

An entity must take all reasonable steps to complete the assessment within **30 calendar days** after the day the entity became aware of the grounds (or information) that caused it to suspect an eligible data breach (s 26WH(2)).

The Commissioner expects that wherever possible entities treat 30 days as a maximum time limit for completing an assessment, and endeavour to complete the assessment in a much shorter timeframe, as the risk of serious harm to individuals often increases with time.

Where an entity cannot reasonably complete an assessment within 30 days, the Commissioner recommends that it should document this, so that it is able demonstrate:

- that all reasonable steps have been taken to complete the assessment within 30 days
- the reasons for the delay
- that the assessment was reasonable and expeditious.

How is an assessment done?

Entities must carry out a 'reasonable and expeditious' assessment (s 26WH(2)(a)). The Privacy Act does not set out how entities should assess a data breach, and entities may develop their own procedures for assessing a suspected breach.

The Commissioner expects that the amount of time and effort entities will expend in an assessment should be proportionate to the likelihood of the breach and its apparent severity.

The Commissioner expects that an entity's approach to data breach management, including its data breach response plan, will incorporate the requirements of the NDB scheme for assessing suspected eligible data breaches.

While the Privacy Act does not specify how an assessment should occur, the OAIC suggests that an assessment could be a three-stage process:

1. **Initiate:** decide whether an assessment is necessary and identify which person or group will be responsible for completing it
2. **Investigate:** quickly gather relevant information about the suspected breach including, for example, what personal information is affected, who may have had access to the information and the likely impacts
3. **Evaluate**: make a decision, based on the investigation, about whether the identified breach is an eligible data breach (see Identifying Eligible Data Breaches).

The Commissioner recommends that entities document the assessment process and outcome.

Remedial action

At any time, including during an assessment, an entity can, and should, take steps to reduce any potential harm to individuals caused by a suspected or eligible data breach. If remedial action is successful in preventing serious harm to affected individuals, notification is not required (as explained in Identifying Eligible Data Breaches).

Breach established — what next?

Once an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach – whether during the course of an assessment, or when the assessment is complete – it must promptly notify affected individuals and the Commissioner about the breach (see What to Include in an Eligible Data Breach Statement and Notifying Individuals About an Eligible Data Breach).

Notifying individuals about an eligible data breach

Key points

- When an entity experiences a data breach, its first step should be to contain the breach where possible and take remedial action. Where serious harm cannot be mitigated through remedial action (see Identifying Eligible Data Breaches), it must notify individuals at risk of serious harm and provide a statement to the Commissioner as soon as practicable.
- If it is not practicable to notify individuals at risk of serious harm, an entity must publish a copy of the statement prepared for the Commissioner on its website, and take reasonable steps to bring its contents to the attention of individuals at risk of serious harm.
- If a single eligible data breach applies to multiple entities, only one entity needs to notify the Commissioner and individuals at risk of serious harm. It is up to the entities to decide who notifies. Generally, the Commissioner suggests that the entity with the most direct relationship with the individuals at risk of serious harm should undertake the notification.

Who needs to be notified?

Once an entity has reasonable grounds to believe there has been an eligible data breach, the entity must, as soon as practicable, make a decision about which individuals to notify, prepare a statement for the Commissioner and notify individuals of the contents of this statement.

The NDB scheme provides flexibility — there are three options for notifying individuals at risk of serious harm, depending on what is 'practicable' for the entity (s 26WL(2)).

Whether a particular option is practicable involves a consideration of the time, effort, and cost of notifying individuals at risk of serious harm in a particular manner. These factors should be considered in light of the capabilities and capacity of the entity.

Option 1 — Notify all individuals

If it is practicable, an entity can notify each of the individuals to whom the relevant information relates (s 26WL(2)(a)). That is, all individuals whose personal information was part of the eligible data breach.

This option may be appropriate, and the simplest method, if an entity cannot reasonably assess which particular individuals are at risk of serious harm from an eligible data breach that involves personal information about many people, but where the entity has formed the view that serious harm is likely for one or more of the individuals.

The benefits of this approach include ensuring that all individuals who may be at risk of serious harm are notified, and allowing them to consider whether they need to take any action in response to the eligible data breach.

Option 2 — Notify only those individuals at risk of serious harm

If it is practicable, an entity can notify only those individuals who are at risk of serious harm from the eligible data breach (s 26WL(2)(b)).

That is, individuals who are likely to experience serious harm as a result of the eligible data breach. If an entity identifies that only a particular individual, or a specific subset of individuals, involved in

an eligible data breach is at risk of serious harm, and can specifically identify those individuals, only those individuals need to be notified.

The benefits of this targeted approach include avoiding unnecessary distress to individuals who are not at risk, limiting possible notification fatigue among members of the public, and reducing administrative costs, where it is not required by the NDB scheme.

Example
An attacker installs malicious software on a retailer's website. The software allows the attacker to intercept payment card details when customers make purchases on the website. The attacker is also able to access basic account details for all customers who have an account on the website. Following a comprehensive risk assessment, the retailer considers that the individuals who made purchases during the period that the malicious software was active are at likely risk of serious harm, due to the likelihood of payment card fraud. Based on this assessment, the retailer also considers that those customers who only had basic account details accessed are not at likely risk of serious harm. The retailer is only required to notify those individuals that it considers to be at likely risk of serious harm.

Option 3 — Publish notification

If neither option 1 or 2 above are practicable, for example, if the entity does not have up-to-date contact details for individuals, then the entity must:

- publish a copy of the statement on its website if it has one
- take reasonable steps to publicise the contents of the statement (s 26WL(2)(c)).

It is not enough to simply upload a copy of the statement prepared for the Commissioner on any webpage of the entity's website. Entities must also take proactive steps to publicise the substance of the eligible data breach (and at least the contents of the statement), to increase the likelihood that the eligible data breach will come to the attention of individuals at risk of serious harm.

While the Privacy Act does not specify the amount of time that an entity must keep the statement accessible on their website, the Commissioner would generally expect that it is available for at least 6 months.

Example
In the process of cleaning up his old desktop, an accountant accidently sends a spreadsheet containing the TFN and contact information of his past clients to his entire email contact list. He is worried that the information contained could be used for identity theft and understands that 'recalling' emails does not usually work. He emails his contact list to request that they immediately delete the spreadsheet and notify him when this has happened. In addition, since the file is over ten years old, he decides that notifying individuals directly (through option 1 or 2) would not be practicable, as their contact details would more than likely be outdated. He notifies the Commissioner about the data breach and publicises a notification (option 3).

How do I notify and what do I need to say?

Options 1 (Notify all individuals) and 2 (Notify only those individuals at risk of serious harm)

Options 1 and 2 above require that entities take 'such steps as are reasonable in the circumstances to notify individuals about the contents of the statement' that the entity prepared for the Commissioner (s 26WL(2)(a) and (b)).

The entity can use any method to notify individuals (for example, a telephone call, SMS, physical mail, social media post, or in-person conversation), so long as the method is reasonable. In considering whether a particular method, or combination of methods is reasonable, the notifying entity should consider the likelihood that the people it is notifying will become aware of, and understand the notification, and weigh this against the resources involved in undertaking notification.

An entity can notify an individual using their usual method of communicating with that particular individual (s 26WL(4)). For example, if an entity usually communicates through a nominated intermediary, they may also choose to notify through this intermediary.

The entity can tailor the form of its notification to individuals, as long as it includes the content of the statement required by s 26WK. That statement (and consequently, the notification to individuals) must include the following information:

1. the identity and contact details of the entity (s 26WK(3)(a))
2. a description of the eligible data breach that the entity has reasonable grounds to believe has happened (s 26WK(3)(b))
3. the kind, or kinds, of information concerned (s 26WK(3)(c))
4. recommendations about the steps that individuals should take in response to the eligible data breach (s 26WK(3)(d)).

Decisions about the appropriate types of recommendations will always be dependent on the circumstances of the eligible data breach. This may include choosing to tailor recommended steps around an individual's personal circumstances, or providing general recommendations that apply to all individuals. In some circumstances, the entity may have already taken some protective steps, reducing the necessity for action by affected individuals. The entity may choose to explain these measures in the notice to individuals as a part of their recommendation. For example, a bank may notify an individual that it has suspended suspicious transactions on their account and recommended steps may be limited to suggesting the individual monitor their accounts and notify the bank immediately of any other suspicious transactions.

Option 3 (Publish notification)

Option 3, which can only be used if options 1 or 2 are not practicable, requires an entity to publish a copy of the statement prepared for the Commissioner on its website, and take reasonable steps to publicise the contents of that statement.

An entity should consider what steps are reasonable in the circumstances of the entity and the data breach to publicise the statement. The purpose of publicising the statement is to draw it to the attention of individuals at risk of serious harm, so the entity should consider what mechanisms would be most likely to bring the statement to the attention of those people.

A reasonable step when publicising an online notice, might include:

- ensuring that the notice is prominently placed on the relevant webpage, which can be easily located by individuals and indexed by search engines
- publishing an announcement on the entity's social media channels
- taking out a print or online advertisement in a publication or on a website the entity considers reasonably likely to reach individuals at risk of serious harm.

In some cases, it might be reasonable to take more than one step to publicise the contents of the statement. For example, if a data breach involves a particularly serious form of harm, or affects a large number of individuals, an entity could take out multiple print or online advertisements (which could include paid advertisements on social media channels), publish posts on multiple social media channels, or use both traditional media and online channels.

The approach to publicising the statement may depend on the publication method. For example, where space and cost allows, an entity may republish the entirety of the information required to be included in the statement. Another option, if the available space is limited, or the cost of republishing the entire statement would not be reasonable in all the circumstances, would be to summarise the information required to be included in the statement and provide a hyperlink to the copy of the statement published on the entity's website. Entities should keep in mind the ability and likelihood of individuals at risk of serious harm being able to access the statement when determining the appropriateness of relying solely on such an approach.

If option 3 is chosen, entities should take care to ensure that the online notice does not contain any personal information. While it may help if entities provide a general description of the cohort of affected individuals, this description should not identify any of the affected individuals or provide information that may make an individual reasonably identifiable. For example, it may be appropriate for an online retailer to publicise that individuals who made transactions in the year 2013 may be affected, but it would not be appropriate for the retailer to publicise the names associated with any compromised transaction data.

Timing of notification

Entities must notify individuals as soon as practicable after completing the statement prepared for notifying the Commissioner (s 26WL(3)).

Considerations of cost, time, and effort may be relevant in an entity's decision about when to notify individuals. However, the Commissioner generally expects entities to expeditiously notify individuals at risk of serious harm about an eligible data breach unless cost, time, and effort are excessively prohibitive in all the circumstances.

If entities have notified individuals at risk of serious harm of the data breach before they notify the Commissioner, they do not need to notify those individuals again, so long as the individuals were notified of the contents of the statement given to the Commissioner. The scheme does not require that notification be given to the Commissioner before individuals at risk of serious harm, so if entities wish to begin notifying those individuals before, or at the same time as notifying the Commissioner, they may do so.

What to include in an eligible data breach statement

Key points

- The NDB scheme requires entities to notify individuals about an eligible data breach (see Identifying Eligible Data Breaches).
- Entities are also required to prepare a statement and provide a copy to the Commissioner (s 26WK). The OAIC's online form may help entities to do this.
- The statement must include the name and contact details of the entity, a description of the eligible data breach, the kind or kinds of information involved, and what steps the entity recommends that individuals at risk of serious harm take in response to the eligible data breach (s 26WK(3))
- Entities must notify affected individuals about the contents of this statement or, if this is not practicable, publish a copy of the statement on the entity's website and take reasonable steps to publicise the contents of the statement (s 26WL(2)) (see Notifying individuals about an eligible data breach).

What must be included in the statement

A statement about an eligible data breach must include:

- the identity and contact details of the entity (s 26WK(3)(a))
- a description of the eligible data breach (s 26WK(3)(b))
- the kind or kinds of information involved in the eligible data breach (s 26WK(3)(c))
- what steps the entity recommends that individuals take in response to the eligible data breach (s 26WK(3)(d)).

Identity and contact details of the entity

Where an entity's company name is different to the business or trading name, the OAIC recommends that entities also include the name that is most familiar to individuals. The entity must also include information about how an individual can contact it. Depending on the nature and scale of the breach, the entity may wish to consider whether to provide its general contact details, or establish a dedicated phone line or email address to answer queries from individuals.

Description of the eligible data breach

An entity is required to include 'a description' of the data breach in its statement.

The OAIC expects that the statement will include sufficient information about the data breach to allow affected individuals the opportunity to properly assess the possible consequences of the data breach for them, and to take protective action in response.

Information describing the eligible data breach may include:

- the date, or date range, of the unauthorised access or disclosure
- the date the entity detected the data breach

- the circumstances of the data breach (such as any known causes for the unauthorised access or disclosure)
- who has obtained or is likely to have obtained access to the information
- relevant information about the steps the entity has taken to contain or remediate the breach.

In general, the OAIC does not expect entities to identify the specific individuals who have accessed information, unless this is relevant to the steps the entity recommends individuals might take in response. For example, where information has been accidentally disclosed in a family violence situation known to the entity, this would be important information for the individual to know.

Usually, however, it would suffice to provide a general description of the type of person who has obtained the information, such as 'an external third party' or 'former employee'.

The kind or kinds of information concerned

The statement must include the kind or kinds of information involved in the data breach. Knowing what kind of personal information has been breached is critical to assessing what action should be taken by individuals following a data breach.

Entities, in assessing the data breach, should clearly establish what information was involved in the data breach, including whether the breach involved 'sensitive information'[28] (such as information about an individual's health), government related identifiers (such as a Medicare number or driver licence number), or financial information.

Steps recommended to individuals in response to the eligible data breach

The statement must include recommendations individuals should take in response to the data breach, to mitigate the serious harm or likelihood of serious harm from the data breach.

The nature of recommendations will depend on the entity's functions and activities, the circumstances of the eligible data breach, and the kind or kinds of information that were involved. Recommendations should include practical steps that are easy for the individuals to action.

For example, to help reduce the risk of identity theft or fraud, recommendations in response to a data breach that involved individuals' Medicare numbers might include steps an individual can take to request a new Medicare card. Or in the case of a data breach that involved credit card information, putting individuals at risk of identity theft, recommendations might include that an individual contact their financial institution to change their credit card number, and also contact a credit reporting body to establish a ban period on their credit report.

Where the entity does not have the requisite knowledge or capacity to provide advice to affected individuals, they should seek specialist advice or assistance in preparing this section. In limited circumstances, after seeking advice, the entity may use this section to advise individuals that no steps are required.

[28] See s 6(1) of the Privacy Act for categories of personal information that are covered by the definition of 'sensitive information'.

Additional information to provide

Other entities involved in the data breach

If more than one entity holds personal information that was compromised in an eligible data breach, only one entity needs to prepare a statement and notify individuals about the data breach (s 26WM, and see Data Breaches Involving More Than One Entity). This may occur when an entity outsources the handling of personal information, is involved in a joint venture, or where it has a shared services arrangement with another entity.

When a data breach affects more than one entity, the entity that prepares the statement may include the identity and contact details of the other entities involved (s 26WK(4)). Whether an entity includes the identity and contact details of other involved entities in its statement will depend on the circumstances of the eligible data breach, and the relationship between the entities and the individuals involved. The Privacy Act does not require this information to be included on the statement, and it is open to entities to assess whether it is useful to provide this information to individuals.

The OAIC recognises that in some instances the identity and contact details of a third party may not be relevant to an individual whose personal information is involved in an eligible data breach, for example, where the individual does not have a relationship with the other entity. In these circumstances, rather than include the identity and contact details of the third party or parties, the entity that prepares the statement may wish to describe the nature of the relationship with the third party in its description of the data breach.

When to provide a copy of the statement to the Commissioner

Entities must prepare and give a copy of the statement to the Commissioner as soon as practicable after becoming aware of the eligible data breach (s 26WK(2)).

What is a 'practicable' timeframe will vary depending on the entity's circumstances, and may include considerations of the time, effort, or cost required to prepare the statement. The OAIC expects that once an entity becomes aware of an eligible data breach, it will provide a statement to the Commissioner promptly, unless there are circumstances that reasonably hinder the entity's ability to do so.

It may be appropriate in some circumstances for an entity to advise individuals about the contents of the statement before or at the same time that it gives the statement to the Commissioner, rather than waiting.

While a statement provided to the Commissioner and individuals must include certain information outlined above (s 26WK(3)), where additional relevant information becomes available after submitting this statement, the entity may provide this to the OAIC. The OAIC will include instructions about how to provide any supplementary information upon receipt of the statement.

How to provide the statement to the Commissioner

The OAIC has an online form for entities to lodge all eligible date breach statements under section 26WK of the Privacy Act.

If you are unable to use the online form, please contact the OAIC enquiries line to make alternative arrangements.

Australian Information Commissioner's role in the NDB scheme

Key points

The Commissioner has a number of roles under the NDB scheme in the Privacy Act. These include:

- receiving notifications of eligible data breaches
- encouraging compliance with the scheme, including by handling complaints, conducting investigations, and taking other regulatory action in response to instances of non-compliance
- offering advice and guidance to regulated entities, and providing information to the community about the operation of the scheme.

This document summarises how the Commissioner anticipates exercising these functions. For more information about the Commissioner's regulatory powers and how those powers are exercised, see the OAIC's Privacy Regulatory Action Policy[29] and the Guide to Privacy Regulatory Action.[30]

Notifications of data breaches to the Commissioner

How to notify the Commissioner

Once an entity has reasonable grounds to believe there has been an eligible data breach and it is not exempted from notifying, it is required to provide notification to individuals at risk of serious harm and the Commissioner. When notifying the Commissioner, the entity must provide a notification statement that contains the following information (s 26WK(3)):

1. The identity and contact details of the notifying entity.
2. A description of the data breach.
3. The kind or kinds of information concerned.
4. Recommendations to individuals about the steps that they should take to minimise the impact of the breach.

An online form is available on the OAIC website to help entities lodge notification statements and provide additional supporting information (see What to Include in an Eligible Data Breach Statement).

Providing voluntary information

Although not required by the Privacy Act, entities may provide additional supporting information to the Commissioner to explain the circumstances of the data breach and the entity's response in further detail. For example, entities may choose to provide the Commissioner with technical

[29] The Privacy Regulatory Action Policy explains the OAIC's approach to using its privacy regulatory powers and communicating information publicly. See the OAIC website <https://www.oaic.gov.au>.

[30] The Guide to Privacy Regulatory Action sets out a detailed explanation of particular privacy regulatory powers, looking at the legislative framework and purpose of the power, and the procedural steps the OAIC will take in the exercise of the regulatory power. See the OAIC website <https://www.oaic.gov.au>.

information, which may not be appropriate to include in the statement to individuals. This information will assist the Commissioner to decide whether to make further inquiries or to take any other action. It may also be used by the Commissioner when preparing statistical reports about notifications received.

When a data breach affects more than one entity, the entity that prepares the statement may also choose to include the identity and contact details of the other entities involved (s 26WK(4)). The Privacy Act does not require this information to be included on the statement, and it is open to entities to assess whether it is useful to provide this information in the statement.

Confidentiality of information provided in notifications

If an entity elects to provide additional supporting information to the Commissioner, it may request that the Commissioner hold that information in confidence. The Commissioner will respect the confidence of commercially or operationally sensitive information provided voluntarily in support of a data breach notification, and will only disclose such information after consulting with the notifying entity, and with the entity's agreement or where required by law.

If the Commissioner receives a freedom of information (FOI) request for a notification statement or additional supporting information, the Commissioner will consult with the entity that made the notification before responding. As a matter of course, the Commissioner will offer to transfer any FOI requests relating to agencies to the agencies in question.

The Commissioner's response to notifications

The Commissioner will acknowledge receipt of all data breach notifications.

The Commissioner may also make inquiries or offer advice and guidance in response to notifications. In deciding whether to make inquiries or offer advice and guidance in response to a notification, the Commissioner may consider the type and sensitivity of the personal information, the numbers of individuals potentially at risk of serious harm, and the extent to which the notification statement and any additional supporting information provided demonstrate that:

- the data breach has been contained or is in the process of being contained where feasible
- the notifying entity has taken, or is taking, reasonable steps to mitigate the impact of the breach on the individuals at risk of serious harm
- the entity has taken, or is taking, reasonable steps to minimise the likelihood of a similar breach occurring again.

The Commissioner may also decide to take regulatory action on the Commissioner's own initiative in response to a notification, or a series of notifications. In deciding whether to take regulatory action, the Commissioner will have regard to the OAIC's Privacy regulatory action policy and Guide to privacy regulatory action.

However, generally the Commissioner's priority when responding to notifications is to provide guidance to the entity and to assist individuals at risk of serious harm.

The Commissioner's enforcement of the NDB scheme

The Commissioner has a number of enforcement powers to ensure that entities meet their obligations under the scheme. A failure by an entity to meet any of the following requirements of the scheme is an interference with the privacy of an individual (s 13(4A)):

- Conduct a reasonable and expeditious assessment of a suspected eligible data breach (s 26WH(2)), taking all reasonable steps to ensure that this assessment is completed within 30 days of becoming aware (s 26WH(2)(b)).
- Prepare a statement about the data breach, and give a copy to the Commissioner, as soon as practicable (s 26WK(2)).
- Notify the contents of the statement to individuals at risk of serious harm (or, in certain circumstances, publish the statement) as soon as practicable (s 26WL(3)).
- Comply with a direction from the Commissioner to prepare a statement and notify as soon as practicable (s 26WR(10)).

The enforcement powers available to the Commissioner in response to an interference with privacy, which range from less serious to more serious regulatory action, include powers to:

- accept an enforceable undertaking (s 33E) and bring proceedings to enforce an enforceable undertaking (s 33F)
- make a determination (s 52) and bring proceedings to enforce a determination (ss 55A and 62)
- seek an injunction to prevent ongoing activity or a recurrence (s 98)
- apply to court for a civil penalty order for a breach of a civil penalty provision (s 80W), which includes a serious or repeated interference with privacy (s 13G). [31]

The Commissioner is also required, in most circumstances, to investigate a complaint made by an individual about an interference with the individual's privacy (s 36), which would include a failure to notify an individual at risk of serious harm of an eligible data breach where required to do so.

In deciding when to exercise enforcement powers in relation to a contravention of the NDB scheme, the Commissioner will have regard to the OAIC's Privacy Regulatory Action Policy and the circumstances outlined in Chapter 9: Data Breach Incidents of the OAIC's Guide to Privacy Regulatory Action.

The preferred approach of the Commissioner is to work with entities to encourage and facilitate compliance with an entity's obligations under the Privacy Act before taking enforcement action.

The Commissioner acknowledges that it will take time for all regulated entities to become familiar with the requirements of the NDB scheme. During the first 12 months of the scheme's operation, the Commissioner's primary focus will be on working with entities to ensure that they understand the new requirements and are working in good faith to implement them.

The Commissioner's other powers and functions under the scheme

Direction to notify (s 26WR)

The Commissioner can direct an entity to notify individuals at risk of serious harm, as well as the Commissioner, about an eligible data breach in certain circumstances.

Before directing an entity to notify, the Commissioner will usually ask the entity to agree to notify. This might happen if a data breach comes to the attention of the Commissioner but has not come

[31] For more information about civil penalty provisions in the Privacy Act, see Guide to Privacy Regulatory Action, Chapter 6: Civil Penalties — Serious or Repeated Interference With Privacy and Other Penalty Provisions.

to the attention of the relevant entity, or if the Commissioner does not agree with the entity's initial view about whether a data breach triggers an obligation to notify.

If the Commissioner and the entity cannot agree about whether notification should occur, the Commissioner will give the entity an opportunity to make a formal submission about why notification is not required, or if notification is required, on what terms. The Commissioner will consider the submission and any other relevant information before deciding whether to direct the entity to notify under s 26WR.

Declaration that notification need not be made, or that notification be delayed (s 26WQ)

The Commissioner may declare that notification of a particular data breach is not required (s 26WQ(1)(c)). The Commissioner may also modify the period in which notification needs to occur (s 26WQ(1)(d)).

The Commissioner cannot make a declaration under s 26WQ unless satisfied that it is reasonable in the circumstances to do so, having regard to the public interest, any relevant advice received from an enforcement body or the Australian Signals Directorate, and any other relevant matter. While the Commissioner is empowered to make a declaration if it is 'reasonable in the circumstances to do so', the Commissioner still has discretion about whether to make a declaration, and on what terms.

In deciding whether to make a declaration, and on what terms, the Commissioner will have regard to the objects of the Privacy Act (s 2A) and other relevant matters. The Commissioner will consider whether the risks associated with notifying a particular data breach outweigh the benefits of notification to individuals at risk of serious harm.

Given the clear objective of the scheme to promote notification of eligible data breaches to affected individuals, and the inclusion of exceptions in the scheme that remove the need to notify in a wide range of circumstances, the Commissioner expects that declarations under s 26WQ will be limited to exceptional cases.

An entity applying for a declaration will be expected to make a well-reasoned and convincing case detailing how the data breach is an eligible data breach, why any relevant exceptions do not apply, and why notification should not occur or should be delayed. The entity should provide detailed evidence or information in support of its application.

Advice, guidance, and community information

The Commissioner provides general information to the community about the Privacy Act, including the NDB scheme, via the OAIC's website or its public enquiries service.

The Commissioner has developed this guide and other resources, which are available on the OAIC's website, to help entities comply with the scheme.

However, the Commissioner will not be able to provide detailed advice about the application of the scheme to specific data breaches. Entities should seek their own legal and technical advice.

Part of the Commissioner's role in the NDB scheme is to promote transparency in the way that entities handle personal information. To this end, the Commissioner will regularly publish de-identified statistical information about data breaches notified under the scheme.

Part 5: Other sources of information

This guide has focussed on how to manage data breaches affecting personal information for entities with obligations under the Privacy Act.

Entities may need to consider whether the circumstances of a data breach triggers other requirements, or if the type of information that they hold warrants specific actions to prepare for and manage a data breach. For instance, it may be appropriate to seek advice from the Australian Taxation Office for a data breach that involves tax file numbers; or to seek guidance from the Australian Digital Health Agency if a data breach involves information stored in the My Health Record system.

Entities may also be required to notify other regulators about certain matters under industry-specific regulation; or to notify professional associations about matters related to a data breach. Contractual arrangements may also create obligations to do certain things to prepare for a data breach, and to share certain information in the event of a data breach.

Relevant sources of advice in the event of a data breach (in addition to the Commissioner) may include:

- federal or State or Territory police or law enforcement bodies
- the affected entity's financial services provider
- Australian Securities & Investments Commission (ASIC)
- Australian Prudential Regulation Authority (APRA)
- Australian Taxation Office (ATO)
- Australian Cyber Security Centre (ACSC)[32]
- CERT Australia
- Australian Transaction Reports and Analysis Centre (AUSTRAC)
- Australian Digital Health Agency (ADHA)[33]
- Department of Health[34]
- State or Territory Privacy and Information Commissioners[35]
- IDcare, or other organisations that support individuals affected by data breaches
- professional associations and professional regulatory bodies
- third parties under an agreement or contract, for example contracted service providers or insurance providers.

---

[32] Further information about cyber security incidents that should be reported is available at <https://www.cyber.gov.au/report>.

[33] For data breaches involving the My Health Record system.

[34] For data breaches involving the National Cancer Screening Register.

[35] For more information about state and territory jurisdictions, see Privacy in Your State, OAIC website <https://www.oaic.gov.au>.

Other OAIC resources

The following resources can be found on the OAIC website <https://www.oaic.gov.au>:

- Guide to Securing Personal Information
- Chapter 9: Data Breach Incidents in the Guide to Privacy Regulatory Action
- Chapter 1 and Chapter 11 of the APP Guidelines
- Consumer resources: Data Breaches
- Guide to Mandatory Data Breach Notification in the My Health Record System

Cyber security resources

Technical standards and guidance that may assist entities to prepare for and respond to a data breach include the following:

- CERT Australia, Australia's national computer emergency response team — CERT Australia provides advice and support on cyber threats and vulnerabilities to the owners and operators of Australia's critical infrastructure and other systems of national interest.
- International standards published by the International Organization for Standardization (ISO) and Australian standards published by Standards Australia, including the AS/NZS ISO/IEC 27000 series of information security management standards
- National Institute of Standards and Technology (USA), provides detailed frameworks based on ISO standards (see Cybersecurity on the NIST website)
- Control Objectives for Information and Related Technology (COBIT) — COBIT 5 is the latest edition of Information Systems Audit and Control Association's (ISACA) international framework for information technology (IT) management and IT governance.
- The National eHealth Security and Access Framework (NESAF) is a comprehensive suite of documents regarding health security for the health industry and specific Australian health organisations. The NESAF aims to assist health organisations in meeting their security obligations.

The following resources are particularly relevant to Australian Government agencies but are also useful for other organisations and government agencies:

- Australian Government Protective Security Policy Framework (PSPF), aims to enhance Australia's information security culture and provide a common approach to the implementation of protective security by Australian Government agencies. The PSPF may also be used by other government agencies (including State and Territory agencies), as well as the private sector as a model for better security practice
- Australian Cyber Security Centre (cyber.gov.au) provides a range of resources on cyber security for businesses, individuals and government, including the Australian Government Information Security Manual and the Essential Eight Maturity Model.

Appendix A: Key terms

'Agency' is defined in s 6(1) of the Privacy Act and includes most Australian Government agencies, agencies and Ministers.

'APPs' are the Australian Privacy Principles set out Schedule 1 to the Privacy Act, which apply to APP entities.

'APP entity' is defined in s 6(1) of the Privacy Act to mean an agency or organisation.

'Assessment' is a key step in responding to a data breach, which should enable entities to make an evidence-based decision about whether serious harm is likely. Entities that are subject to the NDB scheme are required to conduct assessments of suspected eligible data breaches under s 26WH of the Privacy Act.

'Australian Information Commissioner', administers the Privacy Act, and is appointed under s 14 of the Australian Information Commissioner Act 2010 (Cth).

'Credit provider' is defined in s 6(1) of the Privacy Act

'Credit reporting body' is defined in s 6(1) of the Privacy Act and generally applies to a business or undertaking that involves collecting, holding, using, or disclosing personal information about individuals for the purpose of providing an entity with information about the credit worthiness of an individual (s 6P of the Privacy Act).

'Data breach' is the unauthorised access or disclosure of personal information, or loss of personal information.

'Eligible data breach' is the unauthorised access or disclosure of personal information, or loss of personal information in circumstances where this is likely to occur, that is likely to result in serious harm to any of the individuals to whom the information relates (see s 26WE(2) of the Privacy Act).

'Enforcement body' is a body listed in s 6(1) of the Privacy Act.

'Enforcement related activities' are functions listed in s 6(1) of the Privacy Act.

'Entity' is an agency, organisation, credit reporting body, credit provider, or file number recipient that has obligations under s 26WE(1) of the Privacy Act.

'File number recipient' is defined in s 11 of the Privacy Act as a person in possession or control of a record that contains a tax file number.

'Health service' is defined in s 6FB of the Privacy Act, and includes general activities to assess, maintain or improve an individual's health.

'My Health Records Act' is the My Health Records Act 2012 (Cth).

'NDB scheme' is the Notifiable Data Breaches scheme in Part IIIC of the Privacy Act.

'Notifiable data breach' is the same as eligible data breach.

'Notification statement' is a statement about an eligible data breach, prepared by an entity under s 26WK.

'OAIC' is the Office of the Australian Information Commissioner.

'Organisation' is defined in s 6C of the Privacy Act, and includes all businesses and non-government organisations with an annual turnover of more than $3 million, all health service providers and some small businesses (see s 6D and 6E of the Privacy Act).

'Privacy Act' is the Privacy Act 1988 (Cth).

'Personal information' is defined in s 6(1) of the Privacy Act, as information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.

'Remedial action' is the steps that an entity may take to prevent the likelihood of serious harm occurring for any individuals whose personal information is involved in an eligible data breach.

'Sensitive information' is defined in s 6(1) of the Privacy Act to include personal information about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, or criminal record. Sensitive information also includes all health information, genetic information, biometric information that is to be used for the purpose of automated biometric verification or biometric identification, and biometric templates.

'Small business operator' is defined in s 6D of the Privacy Act.

'State or Territory authority' is defined in s 6C(3) of the Privacy Act.

'TFN' means Tax File Number, as defined in s 6(1) of the Privacy Act.

ARIC Workplan July 2024 to June 2025

MEETING		INCLUDED IN BUSINESS PAPER		NOTES
		YES	NO	
1	**Date TBC (July-Sept 2024 Qtr)**			
1.1	External auditor (or their representative) to be invited as an independent observer			
1.2	End of Council term Reports: Four yearly Review of Internal Audit effectiveness by ARIC for Council.			
1.3	End of council term Reports: Four yearly ARIC Committee review by ARIC for Council.			
1.4	End of council term Reports: Four yearly Strategic Assessment by ARIC for Council relating to all matters listed in section 428A of the Local Government Act 1993			
1.5	Review of the Draft Financial Statements.			
1.6	OLG compliance calendar update (6 monthly update)			
1.7	Annual review of the four year Strategic Internal Audit plan			
1.8	ARIC Action List Update (6 monthly)			
1.9	(TBC:) Internal Audit Report: Water Supply (scheduled completion date for Water Supply Audit - June 30 2024 - Ref Paul Quealey email to DCCS 10-11 March 2024)			

MEETING		INCLUDED IN BUSINESS PAPER		NOTES
		YES	NO	
2	**Date TBC (Oct-Dec 2024 Qtr)**			
2.1	Action Plan for most recent Internal Audit			
2.2	External auditor (or their representative) to be invited as an independent observer			
2.3	Annual meeting External Auditor with the Committee (subject to mutually agreeable date)			
2.4	(TBC:) Internal Audit Report - Conflicts of Interest (Ref LSC 4 year Strategic Internal Audit Plan 2022-2025)			
2.5	Advise ARIC of new Councillor member & observer after September 2024 election			
2.6	Audited Financial Statements and Final Audit Management letter.			

MEETING		INCLUDED IN BUSINESS PAPER		NOTES
		YES	NO	
3	**Date TBC (Jan-March 2025 Qtr)**			
3.1	External auditor (or their representative) to be invited as an independent observer			
3.2	Develop 4 year Strategic Internal Audit work plan 2025-2028			
3.3	Review of the EOI for Internal Audit Provider for the 4 year Strategic Internal Audit work plan.			
3.4	(TBC:) Internal Audit Report- Delegations (Ref LSC 4 year Strategic Internal Audit Plan 2022-2025)			
3.5	ARIC Action List update (6 monthly)			
3.6	OLG compliance calendar update (6 monthly update)			
3.7	Action Plan updates for all previous Internal Audits where all agreed actions are not yet complete (annual)			
3.8	Audit Engagement Plan			

MEETING		INCLUDED IN BUSINESS PAPER		NOTES
		YES	NO	
4	**Date TBC (April-June 2025 Qtr)**			
4.1	External auditor (or their representative) to be invited as an independent observer			
4.2	(TBC:) Internal audit Report - Stores (Ref LSC 4 year Strategic Internal Audit Plan 2022-25)			
4.3	Annual review of the Internal Audit function by the ARIC			
4.4	Interim Audit Management letter			
4.5	Annual Attestation Statement by the General Manager - commences with 2024/25 Annual Report			
4.6	Internal Audit Coordinator meeting with the committee			
4.7	Action Plan for most recent Internal Audit			
4.8	Annual review of the ARIC Terms of Reference			

THE COUNTRY MAYORS ASSOCIATION OF NSW INC

"What we want is nothing more than equity"

COMMUNIQUÉ

Country Mayors Association of NSW
Roads and Transport conference Kempsey 12-14 June, 2024

The Country Mayors Association of NSW (CMA) held our Roads and Transports conference from Wednesday 12 to Friday 14 June and Kempsey Shire Councillors and staff were professional and hospitable hosts.

8-9 April 2024. Attendance was under 50, due to numerous conflicting meetings across regional NSW. The conference was held at the Slim Dusty Centre, a facility that the Kempsey Shire is justifiably proud of, having been born from many donations before becoming a Council responsibility.

Kempsey Shire Mayor made us feel welcome at a special function at the Slim Dusty Centre on the Wednesday evening complete with local food and beverages, which included a guided tour of the museum that showcases the life and music of the iconic Aussie, Slim Dusty. Kempsey Shire Mayor, Cr Leo Hauville (below) conducted the welcome and CMA Deputy Chair and Temora Shire Mayor Rick Firman (bottom right) thanked Kempsey on behalf of the CMA.

For further information, contact Cr Jamie Chaffey on 0467 402 412

www.nswcountrymayors.com.au

THE COUNTRY MAYORS ASSOCIATION OF NSW INC

"What we want is nothing more than equity"

COMMUNIQUÉ

The first speaker on the Thursday morning was the Hon Jenny Aitchison, Minister for Regional Transport and Roads and Member for Maitland. The Minister is a friend of the CMA, having fronted up to the past two consecutive CMA meetings. She is pictured bottom right with CMA Executive Member and Narromine Mayor Cr Craig Davies.

Disaster relief was the first topic that the Minister spoke on. She has read the CMA's disaster funding report, so is well aware of the frustrations of Country Councils. The Minister expressed understanding of the stress Councils are under with the cost of disaster recovery, as

For further in

www.nswcountrymayors.com.au

THE COUNTRY MAYORS ASSOCIATION OF NSW INC

"What we want is nothing more than equity"

COMMUNIQUÉ

well as the speed and complexity of funding claims.
"We are trying to get projects started with payment instalments."

"We need to work together with trust, beyond politics. We are focusing on doing the job right. You will see a significant improvement in processing of funding claims in coming months."

Minister Aitchison touch on a pre-budget announcement regarding funding for transport corridors from Port to REZ projects, with over $120mil. earmarked. REZ road network funding involves State and Federal Government collaboration.

In Q&A, Minister Aitchison was asked how untied money for potholes could be attained. She responded that the focus needs to be on disaster relief now and for quite some time to come.
Mayor of Gwydir Shire John Coulton and Mayor of Forbes Shire Phyllis Miller thanked the Minister for her responsiveness.

Bellingen Shire Mayor Steve Allan told the Minister of the $6mil investment into the Bellingen Environment Centre but road infrastructure to it still needs funding. Minister Aitchison said "that is a good example of why we need Integrated Transport Plans, incorporating a range of community stakeholders, with consultation. Toolkits are online for Strategic Regional Transport Plans."

Narrabri Shire Mayor Cr. Darrell Tiemens asked if there has been any progress with the reclassification of roads. The Minister explained "We need to look at these requests on individual merit-based terms. The work on the (reclassification matter) from the previous Government remains sealed.

Member for Oxley, Michael Kemp MP spoke as a proud local and was thanked by CMA Executive Mmeber and Singlton Mayor Cr. Sue Moore (pictured bottom right). The newest politician in the NSW Parliament, the Nationals MP said that Country Mayors are more than roads, rates and rubbish – they are the heart of regional NSW. We need to be open and communicating to work together. The CMA has lobbied so well on many issues from roads to regional crime. The regional crime inquiry and the funding that began in Moree started with the CMA movement. He listed

For further information, contact Cr Jamie Chaffey on 0467 402 412

www.nswcountrymayors.com.au

THE COUNTRY MAYORS ASSOCIATION OF NSW INC

"What we want is nothing more than equity"

COMMUNIQUÉ

rising figures in juvenile and DV crime in the Mid-North Coast. Cost-shifting and the Red Fleet is another area that he supports the removal of, describing it as ludicrous.

CMA Executive Member and Narromine Mayor Cr Craig Davis said that "the Biodiversity Offset Scheme is designed by city people and does not work in our regions. There needs to be more push back by the Nationals. What more can be done to get our message across, where our regional issues are not being heard in the city?"
Mr. Kemp was receptive and advised to take any opportunity to talk to the National Party and make them aware of your concerns.
CMA Executive Member and Armidale Regional Council Mayor Cr Sam Coupland said "We need to change the model for Local Government. We have had to go for 50% SRV. Can we review the system?"
"I am happy to be tied to a position and we need to make it easier for Councils to do their job but I am not aware of a holistic model change on the agenda," responded Mr Kemp.

Shadow Minister for Regional Transport and Roads and Member for Upper Hunter, the Hon. David Layzell had a prior commitment and spoke remotely.

For further information, contact Cr Jamie Chaffey on 0467 402 412

www.nswcountrymayors.com.au

THE COUNTRY MAYORS ASSOCIATION OF NSW INC

"What we want is nothing more than equity"

COMMUNIQUÉ

The regionally based Shadow Minister said that the Country Mayors Association is a fantastic organisation that brings people together and does important work. He described how he built a road in Ghana early in his construction career that mainly involved constructing buildings.

"Roads are so important. Road funding and investment programs such as Fixing Country Roads and the potholes programs have been vital," he said.

Shadow Minister Layzell said "We need to look at improving infrastructure, not just putting things back the same way." He cited examples in the Dungog Shire.

"We have to acknowledge that there are fiscal and inflationary pressures. Managing contractors will never be more important than now. Understand their pressures because we can't lose them."

Mayor of Uralla Shire Council Cr Robert Bell said "Truck drivers pay so many levies and we do not see that money coming out to be spent on our roads."

Shadow Minister Layzell emphasised the importance of trucking freight and roads infrastructure to regional economies.

For further information, contact Cr Jamie Chaffey on 0467 402 412

www.nswcountrymayors.com.au

THE COUNTRY MAYORS ASSOCIATION OF NSW INC

"What we want is nothing more than equity"

COMMUNIQUÉ

Morning tea was a special occasion, with Slim Dusty's daughter Anne Kirkpatrick (a singer-songwriter in her own right) unveiling new museum displays and cutting a 97th birthday cake for Slim.

For further information, contact Cr Jamie Chaffey on 0467 402 412

www.nswcountrymayors.com.au

THE COUNTRY MAYORS ASSOCIATION OF NSW INC

"What we want is nothing more than equity"

COMMUNIQUÉ

Celebrating Country Music history with Anne Kirkpatrick was icing on the cake for CMA Members who enjoyed a very worthwhile event in Kempsey.

Official duties done, Anne posed with CMA members for a group shot.

For further information, contact Cr Jamie Chaffey on 0467 402 412

www.nswcountrymayors.com.au

THE COUNTRY MAYORS ASSOCIATION OF NSW INC

"What we want is nothing more than equity"

COMMUNIQUÉ

Acting CEO of the NSW Reconstruction Authority Mal Lanyon APM and Deputy Secretary – Regional and Outer Metropolitan, Transport for NSW Matt Fuller conducted a panel discussion from the stage after morning tea.

The discussion was open and frank, getting a big thumbs up from the attendees.

"It is important for the Reconstruction Authority to listen. It started December 2022, so it is new and evolving to meet needs. Looking at the transition from emergency to recovery, reconstruction is about the latter," Mal said.

Mal and Matt agreed that the RA and TfNSW need to work better together and assured the CMA that they are working to get things done faster for Councils.

Kempsey Shire Mayor Cr Leo Hauville said "Build back better, like our 56 new bridges. That's the way to go."
Matt: "We are building back better, where necessary, such as the land slip case we saw in Kempsey Shire."
Mal: "We are looking at prioritising investment to high risk areas."

Shoalhaven City Council Mayor Amanda Finlay: We've just had our fifth disaster in four years. We appreciate the collaboration we have but we are still waiting for $15mil and if that does not come in by the end of the financial year, we will be in trouble.
Mal: We accept we need to improve the processing times. We need to shift how we get the money from the Federal Government, so we can release it to Councils faster.
Amanda: Can the Adaption Plans be funded by the Commonwealth?
Mal: The RA will help with them.
Matt: We need open communication to improve our processes.
Ballina Mayor Sharon Cadwallader: We are not cutting down on the red tape. If anything, it has been getting worse. Does the CMA need to advocate more on this politically?
Mal: There is no lack of advocacy. We need to improve and we know that. There will be faster processing in the next month.
Matt: Change is a cultural thing. We acknowledge and that it is needed but it takes time.
Wollondilly Mayor Matt Gould said his council is not disaster declared right now and every council around them has been. Mal said he would look into that.

Gwydir Mayor John Coulton: Councils are ideally placed for determining the cost-effectiveness of betterment versus like for like funding.

For further information, contact Cr Jamie Chaffey on 0467 402 412

www.nswcountrymayors.com.au

THE COUNTRY MAYORS ASSOCIATION OF NSW INC

"What we want is nothing more than equity"

COMMUNIQUÉ

Tenterfield Shire Mayor Bronwyn Petrie: Betterment was the reason for funding refusals from our bushfire damage, including a bridge that was damaged on an important transport road. Re-building what failed is a waste of money.
Mal agreed: We are wasting money.
Matt: We can engage with NEMA and bring diligence and practicality close together.
A southern Council representative offered a road tour to Matt. We (Local Government) are not the enemy.
Matt: We see Councils as partners.

Caption:
CMA Deputy Chairman and Temora Mayor Cr Rick Firman and CMA Executive Member and Forbes Shire Mayor Phyllis Miller are Acting CEO of the NSW Reconstruction Authority Mal Lanyon APM and Deputy Secretary – Regional and Outer Metropolitan, Transport for NSW Matt Fuller

For further information, contact Cr Jamie Chaffey on 0467 402 412

www.nswcountrymayors.com.au

THE COUNTRY MAYORS ASSOCIATION OF NSW INC

"What we want is nothing more than equity"

COMMUNIQUÉ

The Thursday concluded with a bus tour of the new bridges of Kempsey Shire. The most recently completed bridge replacement was officially opened by Minister Jenny Aitchison. Simon Fergusson, a rural-based Kempsey Councillor described the impact of being cut off during recent disasters and the value of the bridge investments. He is pictured below with Member for Oxley Michael Kemp, Kempsey Shire Mayor Cr Leo Hauville and NSW Roads Minister the Hon. Jenny Aitchison. Kempsey Shire's Engineering team look young but have many successful grant applications under their belt but are apparently not available to consult. Their bus replacement tour program is attached.

www.nswcountrymayors.com.au

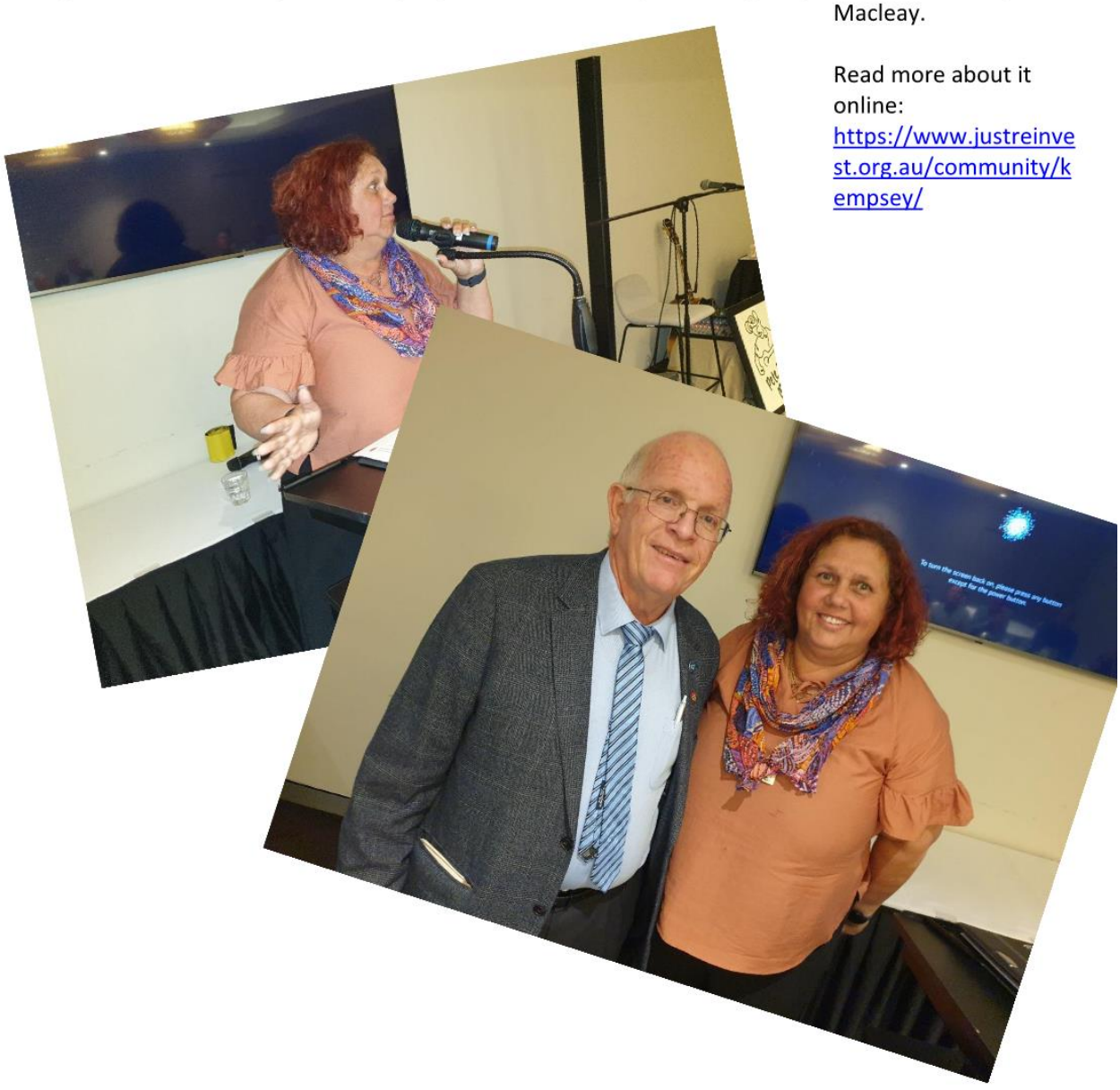
THE COUNTRY MAYORS ASSOCIATION OF NSW INC

"What we want is nothing more than equity"

COMMUNIQUÉ

Kempsey Shire hosted a great conference dinner at the RSL Club, with an inspiring talk by local Aboriginal educator Jo Kelly about the programs she is steering for Aboriginal youth, with Learning the Macleay.

Read more about it online: https://www.justreinvest.org.au/community/kempsey/



For further information, contact Cr Jamie Chaffey on 0467 402 412

www.nswcountrymayors.com.au

THE COUNTRY MAYORS ASSOCIATION OF NSW INC

"What we want is nothing more than equity"

COMMUNIQUÉ

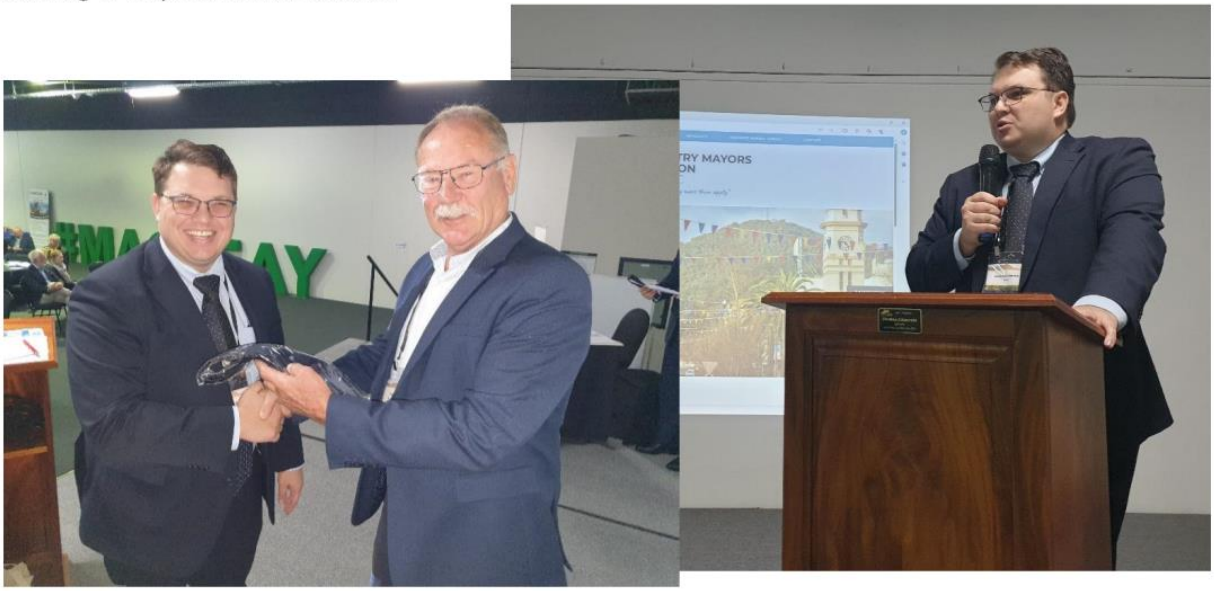
NRMA Policy Advisor, Jonathan Malota was first at the lectern on the Friday morning. He spoke of the NRMA's enthusiasm to work with Country Mayors, to achieve the best possible outcomes with regional roads for road users and local communities.

Mr. Malota condemned the standard of regional roads. He said NRMA members are calling for improvements, adding that there is a $2.35billion backlog in road funding for regional roads p.a. compared to $468mil. in metro areas. "The fact is road funding is not enough," he said.
He detailed the road toll figures and the importance of road safety and road quality.

The NRMA's current and emerging data collection resources was described and he offered to share the data with the CMA and regional Councils, within a formalised relationship. "We want to work with Councils."

Mr. Malota explained that since 2000, all new cars have had a sim card that sends data back to the vehicle manufacturer and NRMA pays a lot of money for that data.
Uralla Mayor Robert Bell asked "can we get this data before it goes to the press, so we can be across it?"

Mr. Malota said Government inefficiencies should be redressed, not tolerated. "Government Departments need KPIs, such as a maximum 30 days to provide an outcome from an application for funding or request further details."



For further information, contact Cr Jamie Chaffey on 0467 402 412

www.nswcountrymayors.com.au

THE COUNTRY MAYORS ASSOCIATION OF NSW INC

"What we want is nothing more than equity"

COMMUNIQUÉ

BusNSW Industry Development Manager Philip Whipp, spoke next and like the industry he represents, he covered a lot of ground. BusNSW is the peak body representing the bus and coach industry in New South Wales and Philip Whipp has been with the organisation since 2016. Prior to that, he held coach company management roles since 2004.
Mr Whipp provided a comprehensive overview of the NSW bus industry, such as the 26,000 accredited bus drivers in NSW – a drop of 11% since Covid. There is a concerning shortage.
There are 660 contracts in regional NSW, which expire in 2026. TfNSW will negotiate with BusNSW regarding the new contracts.

A Bus Industry Taskforce was established in May 2023. Four reports and 58 recommendations resulted. Major reforms expected, including bus driver training. There were recommendations pertaining to Local Traffic Committees in Councils.
Rural and Regional bus contracts - $500mil p.a. funded by the NSW Government.
Cashless, tap and go ticketing system has been trialled in Bathurst and Dubbo but further rollout timeframe is not known.
3,000 zero emission buses are being introduced but the transition will be slow (not likely to be completely rolled out until the 2040s). With a bus expected to have a life of 26-28 years, road maintenance funding is vital to bus operators.
The location of temporary or informal bus stops, such near a farm gate, should involve consultation with Local Councils, according to TfNSW.

Questions related to zero emissions transition and Philip said that it could happen quicker than 2047 in regional areas but did not know if electric buses would impact routes.
Philip Whipp from BusNSW was thanked for his presentation by CMA Executive Member and Tamworth Regional Council Mayor Cr Russell Webb.

For further information, contact Cr Jamie Chaffey on 0467 402 412

www.nswcountrymayors.com.au

THE COUNTRY MAYORS ASSOCIATION OF NSW INC

"What we want is nothing more than equity"

COMMUNIQUÉ

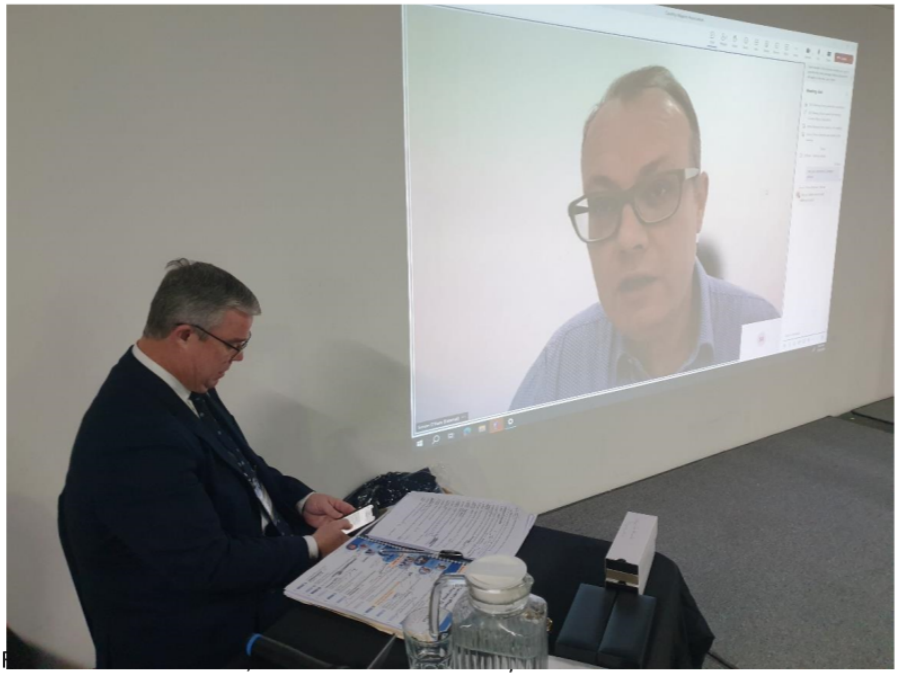
CEO of Road Freight NSW Simon O'Hara spoke next and had to address the conference remotely.
Simon O'Hara is the current CEO of Road Freight NSW, an arm of the Australian Trucking Association. He has years of experience in transport and is admitted as a solicitor in NSW and the High Court of Australia. He has been steering the State's peak trucking industry body since May 2016.
Previously, Simon has held leadership roles in a range of corporations and union type organisations. He has developed strong relationships with Transport for NSW .

Mr. O'Hara said that road transport has faced interesting times, particularly through and post Covid. He described the companies that have a strong relationship with Road Freight NSW, such as Blue Scope Steel. RF NSW has advocated for greater respect for truckies and what they do. There's a complete lack of rest areas in metropolitan NSW.

Inflation rates are coming down but interest rates are not. The demand on the industry has dropped since Covid, especially in the past six months. The demand of agricultural commodities remains strong and road freight is vital to meeting that.

There are drivers leaving the industry and the shortage of drivers is a challenge.
Country roads need to be upgraded. They are an issue for truckies. As are the fees and surcharges at ports.
We are seeing a lot of cost increases and country drivers need to make a living.

"I grew up on a farm near Nullamanna (North of Uralla) for a time during the 70's and early 80's during drought and lived in country towns as well as the city so I understand how, in NSW there is a great deal of focus on metropolitan Sydney. Country Mayors are an important voice and I welcome working with you all!"



www.nswcountrymayors.com.au

THE COUNTRY MAYORS ASSOCIATION OF NSW INC

"What we want is nothing more than equity"

COMMUNIQUÉ

Business Development Manager for Newpave Asphalt, Peter Gellert was a sponsor of the conference. Mr Gellert is proud of the electrical engineering advances he has contributed to the Australian-owned and operated. Established in 2013 in the Hunter region, Newpave has become experts in asphalt manufacturing, construction, testing, haulage, traffic management, profiling, stabilisation and spray seal. Peter has developed a high-tech National Association of Australian State Road Authorities accredited 'roughness' assessing vehicle, an efficient road condition evidence gathering tool.

Mr. Gellert expressed his appreciation for the work of country Mayors and the genuine passion they have for their respective patches.

Mr. Gellert described his electronics background, which led to the road testing and monitoring equipment he has developed. He then detailed what exactly goes into the asphalt and spray seal that his company produces and the processes involved.

His presentation is attached.
Peter Gellert was thanked for his contribution by Kempsey Shire Mayor Cr. Leo Hauville.

For further information, contact Cr Jamie Chaffey on 0467 402 412

www.nswcountrymayors.com.au

THE COUNTRY MAYORS ASSOCIATION OF NSW INC

"What we want is nothing more than equity"

COMMUNIQUÉ

The final speaker at the conference was UGL Regional Linx Network Operations Manager, Mitch Scealy. UGL Regional Linx manages all infrastructure and maintenance on the Country Regional (rail) Network in NSW. This network ensures the safe movement of people and goods throughout the regions of NSW, and links Sydney with many important regional centres.

Based in the Central West, Mr Scealy has rail tracks in his blood. His father has been working in the railways for 50 years. The rail infrastructure that UGL Regional Linx is responsible for includes the historic landmark train stations in our regional centres. It also faces challenges with infrastructure that is no longer used, such as the Sunnyside timber rail bridge in the Tenterfield Shire, which Mayor Bronwyn Petrie asked about.

Unfortunately, Mr. Scealy said that the heritage listing of the Sunnyside bridge and other such structures can mean it is difficult to address concerns, regardless of how dilapidated they may be.

Mr Scealy said that UGL Regional Linx looks forward to building its relationship with the Country Mayors Association of NSW into the future.

His presentation is attached.

He was thanked by CMA Deputy Chairman and Temora Shire Mayor Cr Rick Firman, who was MC for the conference.

For further information, contact Cr Jamie Chaffey on 0467 402 412

www.nswcountrymayors.com.au

THE COUNTRY MAYORS ASSOCIATION OF NSW INC

"What we want is nothing more than equity"

COMMUNIQUÉ

The CMA Executive looks forward to our 9 Aug. 2024 meeting at NSW Parliament.

For further information, contact Cr Jamie Chaffey on 0467 402 412

www.nswcountrymayors.com.au

Cherise Small

Subject: FW: Heritage Grant

From: Denis Doyle <ddoy9194@bigpond.net.au>
Sent: Sunday, 23 June 2024 10:08 AM
To: Greg Tory <Greg.Tory@lachlan.nsw.gov.au>
Subject: Heritage Grant

Good morning Greg

Jeanette and I once again sincerely thank the Lachlan Shire Council for their generous support in the Manse project with the LCS Heritage Grant

Kind regards

Denis and Jeanette Doyle

Denis Doyle Constructions Pty Ltd

ABN 66 130 294 647
Licence No 207761C
33 Craft Crescent Condobolin NSW 2877
Mobile: 0428 952 096
Email: ddoy9194@bigpond.net.au

Mr Greg Tory
General Manager
Lachlan Shire Council
58-64 Molong Street
Condobolin NSW 2877
Australia

Dear Greg

Telstra will soon be closing our 3G network. In the lead up to this, we are upgrading our mobile network in areas that only have Telstra 3G coverage to ensure the same or better 4G coverage is available.

Your area is now Telstra 4G ready.

I'm pleased to let you know that our program of work to deliver this in the Lachlan local government area is now complete, meaning the area is 4G ready. Simply put, if residents could only get 3G on the Telstra network before, they should now be able to enjoy the extra speed and capacity that 4G brings and will continue to have Telstra mobile coverage after the 31st of August.

What you need to do

We know that most our customers' mobile devices in the Lachlan Shire can access the 4G network. However, locally there are still a small number of 3G-only mobile devices accessing our network that will need to be replaced or upgraded before this time if they wish to remain connected.

It is important to note such devices may not be limited to phones and may also include 3G only Telstra Cel-Fi GO Repeaters, 3G only Telstra Mobile Smart Antennas (TMSA), and Internet-of-Things (IoT) or Machine-to-Machine (M2M) devices such as EFTPOS, telemetry & medical devices.

The easiest way to check if mobile phones will be impacted is to use Telstra's free 3G SMS Checker. This tool will show customers who use the Telstra mobile network if their mobile phone is impacted by the 3G network closure, and if so, any action they need to take.

The SMS checker tests the service number you are texting from. If customers simply text the number '3' to 3498, we'll text you back telling you if you need to take any action.

Please note: This checker only works for people using mobile devices who are Telstra customers or are on another supplier who use the Telstra network. For people using Optus or Vodaphone based networks, they will need to check with their carrier if any action is needed.

Some older 4G mobile phones require a 3G network to make calls to Triple Zero, however they use the 4G network for all other calls. This 3G only emergency connectivity is a hardware feature built into the design of the phone by the manufacturer and it is a global, industry-wide issue that many countries have already worked through as they have closed their 3G networks.

Over recent months we have been contacting customers we have been able to identify as using one of these devices to let them know they will likely need to upgrade. Using the SMS checker will help customers confirm if they are potentially impacted.

Customers can also visit our website at https://www.telstra.com.au/support/mobiles-devices/3g-closure for more information and support on device compatibility.

There will be no loss of 3G coverage prior to 31st August 2024. Once we have closed the 3G network, we will repurpose the spectrum so that we can use it to expand our 5G network. We are committed to continuing our long tradition of investment in rural and regional Australia by providing more state-of-the-art services and this is an important step to transition to 5G.

If you or members of your community have any questions about the closure of our 3G network or the steps to take before 31st August 2024, please visit our website.

https://www.telstra.com.au/exchange/our-3g-closure-in-2024--your-questions-answered

Kind regards

Chris Taylor
Regional General Manager (ACT & Sth NSW)
Telstra

RESOURCE STRIPPING at Condobolin / Gilganndra / Coonabarabran "Multi-Purpose Services" (previously "Hospitals")

Timothy Bailey (Nepean Blue Mountains LHD) <Timothy.Bailey@health.nsw.gov.au>
Tue 25/06/2024 01:06

To:barwon@parliament.nsw.gov.au <barwon@parliament.nsw.gov.au>
Cc:Timothy Bailey (Nepean Blue Mountains LHD) <Timothy.Bailey@health.nsw.gov.au>

Dear Mr Butler

I am a doctor who regularly visits (and works in Emergency Departments of) health services within your extraordinarily wide-spread electorate. In addition to those mentioned above, I have also worked recently at Broken Hill Health Service and Narrabri Health Service. My main field of expertise is Emergency Medicine, but I am also well acquainted with General Practice, and Medical Administration - having worked in those areas for several years as well.

The particular foci of my contact today are the three multi purpose services (MPS's) mentioned in the title line above. Today (and for the next week) I am working at Condobolin. I have just completed a ward round and I am confronted with several elderly people who are in need of physiotherapy input, so they can remobilise well enough to get back to their homes.

There is NO AVAILABILITY of physiotherapy services at this facility. This situation is shared with the other MPS's mentioned above, although some of those have a 'virtual physiotherapist' available on a link. The model there is for a centrally-located physiotherapist to instruct a physiotherapy aide, who is located in the peripheral hospital. The aide then assists with mobilising people who are elderly, and/or recovering from injuries. Most of these people are referred back from larger hospital (eg.Orange, Bathurst, RPAH, Dubbo etc.) to have the less specialised inputs provided prior to sending them back home.

Unfortunately, as you can tell from the above, the proposed 'less specialised inputs' to be provided (including physiotherapy) are usually, simply not available at the sites which the patients are referred back to.

The particular story for Condobolin, as far as I am aware, is roughly as follows. Last year the then-existing physiotherapist took maternity leave. On her return, she found her position had been reduced to 0.5 FTE (from full time). The remainder of the physiotherapy allocation for the facility had been 'reallocated' to a 'virtual position'. Subsequently she left the area (possibly due to the lack of full time employment) and the facility advertised for a half-time position to be filled.

After three advertising cycles which were all unsuccessful, the Facility Manager became aware of a physiotherapist who had moved into the area and was keen to find employment in Condobolin. When the Manager applied for permission to advertise again, she was informed that the remaining on-site 0.5FTE had also been 'absorbed' into the 'virtual physiotherapy service'. However, there is no physiotherapy aide at Condobolin now and at any rate, the facility has been informed that they do not qualify for access to the 'virtual physiotherapy' service.

The result is that the people of Condobolin do not have any access to physiotherapy to assist with their mobilisation out of hospital. As a result they remain in hospital for far longer than they should; they are far more likely to end up taking a nursing home bed than they should be; and on discharge from hospital they are both further from their optimal recovery stage than they should be, and more likely to return to hospital. Hardly a QUALITY outcome, or an economically or socially acceptable one.

The bigger picture here is that, in my opinion, and based on my continuing observations of peripheral facilities, they are being comprehensively de-resourced. Those resources are being made increasingly

unavailable to the people in these areas, while many of those people as you know, are working extraordinary hours and in very challenging conditions, year after year, to the benefit of NSW and Australia, and to the disbenefit of themselves. In addition, it seems that now their basic health infrastructure is also being removed.

My reason for writing to you is in the hope that you may be able to make some enquiries on this particular issue, ie. the removal of physiotherapy funding from peripheral hospitals. The peripheral hospitals are getting an increasing load of people from more central facilities, who are transferred for rehabilitation services after specialty inputs at larger hospitals. These transfers are in addition to the local services which would normally be expected to be utilised on more locally based issues, but the peripheral hospitals are being de-resourced and are no longer able to provide the services which are requested of them. I am hoping that this situation may be reversed, either by re-allocating physiotherapy positions to peripheral hospitals, or by recruiting additional physiotherapy aides who will then be able to be instructed by a 'virtual' physiotherapist.

If you can assist with this issue I will be most appreciative, as will those who work and live in Condobolin. Please feel free to make contact at any time.

Regards

TIM BAILEY
BMed; MPH; MRACMA
mob: 0427 478 874

Timely
- Transport out of Condobolin (and all other regional hospitals), for patients with more complex (higher acuity conditions) IS promised, but very rarely achieved.

CONTRIBUTING REASONS: Not enough acute care beds in the state
Not enough ambulance (retrieval) services in the state
Too few penalties for people who abuse ambulance services
No cost for GP attendances to Emergency Depts.

The Hon Paul Scully MP
Minister for Planning and Public Spaces

Ref: IRF24/1443

Cr Paul Phillips
Mayor
Lachlan Shire Council
58-64 Molong Street
Condobolin NSW 2877
council@lachlan.nsw.gov.au

Dear Mayor

As you are aware, the NSW Government is taking immediate action to meet our commitment under the National Housing Accord to build 377,000 new well-located homes by June 2029 to help address the housing crisis.

Local government are a critical enabler of housing, assessing about 85 per cent of housing development applications (DA) in NSW. However, over the past two years, average council DA timeframes have increased by 37 per cent, from 83 in FY21/22 to 114 days in FY23/24, which is contributing to the delays in housing completions and costing the NSW economy at least $89 million each year.

In line with the beginning of the National Housing Accord, and our shared commitment to addressing the housing crisis, I am providing an updated Ministerial Statement of Expectations Order planning.nsw.gov.au/statement-of-expectations-order.

This new Statement of Expectations sets out expectations for council performance in the areas of development assessment, planning proposals and strategic planning. The performance of councils in meeting this Statement of Expectations will be monitored and reported publicly, as will the Department of Planning, Housing and Infrastructure's timeframes for approval of planning proposals and state significant development.

Addressing the housing crisis is a shared responsibility, and all levels of government must do more.

52 Martin Place Sydney NSW 2000
GPO Box 5341 Sydney NSW 2001
02 7225 6080
nsw.gov.au/ministerscully

The Government is also developing a program to support councils achieve local housing targets, reduce average DA timeframes and deliver more homes. We have started this through initiatives funding cadetships for planners in councils and opening a new TAFE course for para-planning. We've completed substantial work on the NSW Planning Portal and are introducing artificial intelligence to support further efficiencies in the local DA process and timely decision-making.

The attached document outlines the key performance metrics within the Statement of Expectations and the associated infrastructure grant funding program. Additional initiatives to support councils achieve faster assessments will be announced in the coming months to help local and State government deliver approvals and particularly homes more effectively.

With these measures, I am confident that councils in NSW can achieve a significant reduction in average DA timeframes and meet our Housing Accord commitments.

I appreciate your leadership and support for this critical work in the spirit of shared responsibility that underpins the National Housing Accord and I look forward to working with you and all councils across New South Wales to deliver more housing for our communities.

Yours sincerely

Paul Scully MP
Minister for Planning and Public Spaces

03/07/2024

Attachment A

This Attachment provides an overview of the initial programs the NSW Government is proposing to support councils in determining more housing-related planning matters during the period of the National Housing Accord. More details of these programs and initiatives will be released in the coming months.

Updated Statement of Ministerial Expectations

- The Ministerial Statement of Expectations establishes the planning-related expectations of the Minister for Planning and Public Spaces in terms of planning assessment performance. The updated Statement includes the expectation for councils to:
    - lodge DAs as soon as practical and within an average of:
        - 14 days from submission, from 1 July 2024 to 30 June 2025
        - 7 days from submission, from 1 July 2025 onwards
    - determine DAs as soon as practical and whichever is the lesser of council's previous financial year average, or an average of:
        - 115 days from lodgement, from 1 July 2024 to 30 June 2025
        - 105 days from lodgement, from 1 July 2025 to 30 June 2026
        - 95 days from lodgement, from 1 July 2026 to 30 June 2027
        - 85 days from lodgement, from 1 July 2027 onwards
    - assess Regionally Significant DAs and refer them to the relevant planning panel for determination as soon as practical and within an average of 250 days from lodgement.

Department of Planning, Housing and Infrastructure Performance

- To assist with delivering major housing projects, the Department will be required to determine State Significant DAs for infill affordable housing and housing in transport-oriented development precincts within an average of 275 days from lodgement.
- As per the LEP Making Guidelines (August 2023) the Department must collaborate with councils to finalise planning proposals in 140 business days for basic proposals, 225 business days for standard proposals, 300 business days for complex proposals, and 380 business days for principal proposals.

Resourcing and financial incentives

- The Department will establish a new $200 million grant program that provides milestone payments to councils based on their performance in meeting the Statement of Expectations. These grants will be for use in improving critical local infrastructure.

- The Department has made $5.6 million worth of funding for grants to councils to integrate AI and other digital solutions into the development assessment process.
- The Department is working with industry, local government and the private sector to support a skilled planning workforce through the Strong Start mentoring program as well as a new TAFE pathway into the planning profession.

Cherise Small

Subject: FW: Mock Crash 2024
Attachments: Mock Crash Invite 2024.pdf

Good Afternoon,

I am emailing you to invite Greg Tory, Adrian Milne, Stephen Taylor, Mayor Paul Philips and Councilors to

NOT A STATISTIC! Youth Driver Education Program's live demonstration (Mock Crash 2024)

At Parkes High School's MPC (entry via the gate on Goobang Street)
Commencing at 9:45am

Please RSVP by Wednesday 7 August 2024 to melanie.suitor@parkes.nsw.gov.au

PSC Engineering

Parkes Shire Council | Wiradjuri Country
2 Cecile Street (PO Box 337), Parkes NSW 2870
engineering@parkes.nsw.gov.au
www.parkes.nsw.gov.au

Parkes Shire Council

NOT A STATISTIC!

YOUTH DRIVER EDUCATION PROGRAM

You are invited to the NOT A STATISTIC!
Youth Driver Education Program's live demonstration

Monday 12 August 2024
Parkes High School's MPC
(entry via the gate on Goobang Street)
Commencing at 9.45am

Please RSVP by Wednesday 7 August 2024 to
Melanie.Suitor@parkes.nsw.gov.au or 6861 2364

NOT A STATISTIC!
MOCK CRASH DEMONSTRATION
YOUTH DRIVER EDUCATION PROGRAM

Parkes Shire Council

FORBES SHIRE COUNCIL

LACHLAN SHIRE COUNCIL