Data Breach Response Plan

Policy Number	A2
Responsible Officer(s)	Chief Executive Officer; Manager People & Governance.
Policy Adopted	October 2023
Next Review Date	October 2027
Minutes reference	2023/10-07
Applicable Legislation	*Privacy Act* (Cth) *1998; Privacy Amendment (Notifiable Data Breaches) Act* (Cth) *2017; South Australian Information Privacy Principles Instruction (Premier and Cabinet Circular PC012 May 2020)*.
Related Policies	Cyber Security Governance Policy; ICT Acceptable Use Policy; Records Management Policy; Risk Management Policy.
Related Documents	Data Breach Response Checklist.

1. PURPOSE

The purpose of this is to plan is to enable Council to respond quickly to a data breach or suspected data breach. By responding quickly, Council can substantially decrease the impact of a breach on affected individuals, reduce the business impacts associated with the breach, and maintain public trust and confidence. The plan also assists Council to meet its legal obligations to maintain data privacy.

2. KEY LEGISLATIVE AND REGULATORY REFERENCES

- *Privacy Act (Cth) 1988* and *Privacy Amendment (Notifiable Data Breaches) Act 2017*. Applies only to particular personal information managed by Council including Tax File Numbers.

- *South Australian Information Privacy Principles Instruction (Premier and Cabinet Circular PC012 May 2020).* Note does not apply to Council.

Note: This Data Breach Response Plan has been developed in consideration of the *Information Privacy Principles* described within both of the above.

3. RELATED COUNCIL POLICIES AND PROCEDURES

- Cyber Security Governance Policy, October 2023
- ICT Acceptable Use Policy, October 2023
- Information Privacy Policy, January 2023
- Records Management Policy, February 2023
- Risk Management Policy, July 2018

4. WHAT IS A DATA BREACH?

A data breach occurs when personal information **that is not already publicly available** is lost or subject to unauthorised access, use, modification or misuse.

Examples include accidentally emailing personal information held by Council, loss of a laptop or mobile phone containing personal information, or a cyber security breach such as a ransomware attack.

5. PERSONAL INFORMATION

Personal information is information or an opinion, whether true or not, relating to a natural person, or the affairs of a natural person, whose identify is apparent, or can reasonably be ascertained. A natural person in this context is a living human being.

Personal information can include combinations of name, address, date of birth, financial or health details, ethnicity, gender, religion, social media, tax file numbers, CCTV recordings, property details, social support details, etc. Personal information may be in paper form, verbal or through electronic means.

The types of personal information controlled by Council and the associated risks and controls required have been identified through Privacy Impact Assessment reviews.

Electronic personal information is stored or accessible in many locations including but not limited to:

- Local IT infrastructure and applications e.g. Local storage devices, servers, Synergy application;
- Cloud based IT systems e.g. Microsoft email, offsite backup;
- IT systems provided by State or Federal Government systems e.g. Dogs and Cats Online, Planning;
- Portable electronic devices e.g. tablets, mobile phones, laptops, USB drives, hard drives;
- IT service provider systems;
- Working from home systems.

6. CAUSES OF DATA BREACHES

A data breach may be caused by malicious action (by an external or inside party), human error, or a breach of cyber security or physical security. A data breach may be actual or suspected and both should be treated similarly as in some cases it may not be possible to confirm that a breach has occurred.

7. ROLES AND RESPONSIBILITIES

Roles and responsibilities within this response plan are as follows:

All Council Members, employees, contractors and volunteers are responsible for:

- Taking reasonable measures to ensure any personal information held by council is protected; and
- Immediately notifying known or suspected data breaches to the Communications & IT Officer.

The Manager People & Governance is responsible for implementation of the Data Breach Response Plan and coordinating Council's response to known data breaches, and suspected data breaches, including forming an appropriate response team if necessary.

The Chief Executive Officer is responsible for determining whether it is necessary to notify parties affected by a data breach or a suspected data breach.

8. REDUCING THE RISK OF ELECTRONIC DATA BREACHES

Privacy risks are integrated within Council's Risk Management Framework.

Council has implemented a range of control measures to reduce the likelihood and impact of data breaches including but not limited to:

- Privacy Breach Impact Assessment;
- Cyber Security Governance Policy;

- ICT Acceptable Use Policy; and
- Data Breach Response Plan (this document).

9. ENCOURAGE REPORTING OF DATA BREACHES

Council Members and the Council CEO shall encourage the reporting of all data breaches, or suspected data breaches in accordance with the procedures in this plan.

In cases where breaches have arisen from a genuine mistake no adverse action shall be taken against the person involved in, or reporting, the incident**.**

10. RANSOMWARE DEMANDS

It is Council policy not to pay ransomware demands.

11. RESPONSE TO A DATA BREACH

If a data breach, or suspected data breach, occurs the following key actions are required to be undertaken by the response team:

Contain

- Contain the breach as soon as possible in order to prevent potential for further compromise of personal information.
- Advise Council's IT service provider if an IT related breach (currently New Era Technology).
- Collect and write down information concerning the circumstances of the breach that may be helpful in later investigations e.g. precise date and times, location, IT systems accessed, technical information, etc. If possible, take a screen shot, mobile phone photo or video of any evidence.
- If the data breach may be a result of criminal actions the Police should be notified as soon as practicable.
- If the Data Breach involves a South Australian Government Agency IT system, advise the relevant agency.
- If the data breach involves an IT system or application provided by a private supplier advise the relevant supplier immediately.

Assess

- Assess the risks of harm to individuals arising from the breach and how the impacts can be mitigated.
- Council's Privacy Breach Impact assessment previously undertaken will assist in the assessment process.
- Seek external advice as required to assess risks and potential remediations.
- Make a determination as to whether serious harm has occurred to individuals and whether this can reasonably be remediated.
- Continue to take available remedial actions to reduce risk of harm.

Notify

- Notify individuals affected if the Chief Executive Officer determines this is required (due to risk of serious harm to individuals that is unable to be remediated).

- If the data breach relates to a Tax File Number, notify individuals and the Australian Information Privacy Commissioner in accordance with the Notifiable Data Breaches Scheme (refer below). This notice is required within 30 days.

Review

- Review the incident within 14 days and consider what actions can be taken to prevent future breaches.

It is recommended these actions are taken simultaneously or in quick succession. **It is very important to act quickly to address a breach**.

12. DATA BREACH RESPONSE CHECKLIST

The attached Data Breach Response Checklist can be used to assist in managing responses and recording actions.

13. DATA BREACH INVOLVING A TAX FILE NUMBER

In accordance with requirements of the Office of the Australian Information Privacy Commissioner, an Eligible Data Breach occurs when the following criteria are met:

- There is unauthorised access to or disclosure of personal information held by Council (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.
- Council has been unable to prevent the likely risk of serious harm with remedial action.

If an Eligible Data Breach occurs Council must report it to the Office of the Australian Information Commissioner in accordance with the instructions available at the OAIC web site as follows:

https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach/

Reporting is required within 30 days.

If an Eligible Data Breach it must also be notified to individuals to whom the information relates.

14. SOUTH AUSTRALIAN GOVERNMENT AGENCIES

Most South Australian Government agencies are required to comply with the South Australian Information Privacy Principles Instruction – Premier and Cabinet Circular PC012. These requirements **do not** apply to Council or Local Government. There is no specific South Australian legislation in relating to information privacy in Local Government.

If a data breach or suspected data breach occurs in relation to personal information held or controlled by a South Australian Government agency notify that agency immediately. The agency is then required to manage the breach with cooperation from Council. South Australian Government agencies are also required to report data breaches to the Privacy Committee of South Australia.

15. REVIEW AND TESTING

Scenario based testing/rehearsal of this Data Breach Response Plan shall be undertaken by Council to facilitate rapid response to mitigate impact in event of an incident.

16. PRIVACY REFRESHER TRAINING

Council shall provide appropriate refresher training to ensure awareness of privacy issues and obligations is maintained.

17. FURTHER GUIDANCE

Council has aligned its Data Breach Response Plan with the recommendations of the Office of the Australian Information Commissioner. Further information is available at the following web site:

https://www.oaic.gov.au/privacy

18. REVIEW

This Policy shall be reviewed every 48 months, or more frequently if required by legislation or Council.

Document history:

Version	Adopted	Description of Change
1.0	October 2023	New Plan