Integrity, Respect, Teamwork, Accountability and Excellence

Cessnock City Council
Data Breach Management Protocol

Date Adopted: **10/11/2023** Revision: **4**

Contents

DISCLAIMER
The information contained in this publication is based on knowledge and understanding at the time of the adoption date, and may not be accurate, current or complete at the time of viewing. While every effort has been made to ensure the accuracy of the information in this publication, Cessnock City Council expressly disclaims any liability to any person in respect of anything done or not done as a result of the contents of this publication or the data provided therein. Readers should make their own inquiries and rely on their own advice when making decisions related to material contained in this publication.

NOTICE © Cessnock City Council
This work is copyright. It may be reproduced in whole or in part for study or training purposes subject to the inclusion of an acknowledgement of the source. It may not be reproduced for commercial usage or sale. Reproduction for purposes other than those indicated above requires written permission from Cessnock City Council.
Council acknowledges Aboriginal people as the traditional custodians on the land on which Cessnock City Council offices, facilities and operations are located, and pay our respects to Elders past, present and future.

1. PROTOCOL OBJECTIVES

The objectives this protocol sets to achieve are to:

1.1. Provide guidance to Council Officials in the event of a Data Breach of information held by Council;

1.2. Set the minimum expectations to be met and practices to be followed by Council to ensure compliance with the obligations and responsibilities set out in Part 6A of the PPIP Act for the mandatory notification of data breach scheme.

2. PROTOCOL SCOPE

2.1. This protocol applies to all Council Officials.

2.2. As the head of the agency, the General Manager is authorised to manage breaches in accordance with section 59ZJ of the PIPP Act and by virtue of their 'Instrument of Sub-Delegation'. The General Manager sub-delegates the performance of functions to manage to data breaches in accordance with this protocol, the Guideline and 59ZJ of the PIPP Act.

2.3. This protocol and its Guideline apply to Personal Information only in the context of managing Data Breaches. Council's Privacy Management Plan takes precedence when dealing with Personal Information in any other context.

2.4. In this protocol a reference to Personal Information is also a reference to Health Information.

3. PROTOCOL STATEMENT

In carrying out its functions and operations, and services, Council collects Personal Information. Council is committed to safeguarding against Data Breaches and to protecting the privacy of individuals. Effective management of Data Breaches assists Council in avoiding or reducing possible harm to affected individuals, organisations and Council itself, assists Council with meeting its responsibilities as a data custodian, and may prevent future breaches.

4. COUNCIL'S PREPAREDNESS

Training and awareness

4.1. To develop a strong front-line defence against Data Breaches and other privacy risks, Council is committed to building a well-trained and aware workforce. To achieve this, Council conducts routine and targeted privacy, Data Breach and cyber security training. This training is provided to all staff.

4.2. Current cyber threat trends are monitored by IT staff who then communicate alerts to staff and/or Councillors when appropriate.

4.3. General privacy awareness training is provided to staff upon their commencement with Council about the responsibilities of identifying, reporting and managing Data breaches. Communications are also relayed to staff periodically and general awareness is published on Council's Intranet.

Processes for identifying and reporting breaches

4.4. To improve the chances of containing Data Breaches and with that potential harms, Council is committed to implementing multilayered technical controls to protect data loss. This includes, but is not limited to:

4.4.1. Use of anti-malware, vulnerability detection, honeypot and firewall systems;

4.4.2. constant monitoring of critical information system resources to automatically alert when suspicious behaviour is detected;

4.4.3. regular internal and external audits which assist Council's practices and processes reflect best industry standards.

4.5. Any suspected or actual Data Breaches must be reported to the Privacy Contact Officer or their delegate/nominee as soon as practically possible. Data breach reporting is to be via a Data Breach CRM or alternatively, by calling Council and asking to speak with the Privacy Contact Officer.

4.6. The Privacy Contact Officer (Director Corporate and Community Services) is the General Manager's delegate and is authorised to deal with Data Breaches in accordance with this protocol, the Guideline and relevant legislation.

Appropriate provisions in contracts and other collaborations

4.7. Council is committed to including provisions in relation to the parties' responsibilities around privacy and Data Breaches prescribed by the PPIP Act when it enters into agreements with other organisations or outsources functions.

4.8. Council uses industry tools to benchmark an organisation's cyber security systems prior to entering into supply contracts.

Testing, currency and alignment

4.9. Council is committed to annual testing of its Data Breach response to ensure relevant staff understand their roles and responsibilities, and to verify that the details (contact numbers, reporting lines, approval processes, etc.) are up to date.

4.10. Testing will involve a role-play exercise to review of how Council staff manage a hypothetical Data Breach. The testing will take into consideration compliance with Council's Privacy Management Plan and will be in line with Council's Cyber Security Plan.

5. RESPONDING TO A DATA BREACH

What is a Data Breach?

5.1. A Data Breach essentially occurs when information Council holds is subject to unauthorised access, disclosure or is lost to circumstance where loss is likely to result in unauthorised access or disclosure.

5.2. Each Data Breach should be assessed on a case-by-case basis but some examples of Data Breaches include:

5.2.1. <u>Human error</u>

i. When a letter or email is sent to the wrong recipient.

ii. When system access is incorrectly granted to someone without appropriate authorisation.

iii. When a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information is lost or misplaced.

CESSNOCK CITY COUNCIL
Integrity, Respect, Teamwork, Accountability and Excellence

iv. When staff fail to implement appropriate password security, for example not securing passwords or sharing password and log in information

5.2.2. System failure

i. Where 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.

ii. Where systems are not maintained through the application of known and supported patches.

5.2.3. Malicious or criminal attack

i. Cyber incidents such as ransomware, malware, hacking, phishing or brute force access attempts resulting in access to or theft of personal information.

ii. Social engineering or impersonation leading into inappropriate disclosure of personal information.

iii. Insider threats from agency employees using their valid credentials to access or disclose personal information outside the scope of their duties or permissions.

iv. Theft of a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information.

What is an Eligible Data Breach?

5.3. An Eligible Data Breach occurs when:

5.3.1. There is unauthorised access to, or unauthorised disclosure of, Personal Information held by Council 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 (***affected individual***), or

5.3.2. Personal Information held by Council is lost in circumstances where:

i. Unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and

ii. If the unauthorised access to, or unauthorised disclosure of, the information was to occur, a reasonable person would conclude that the **ac**cess or disclosure is likely to result in serious harm to the affected individual.

Response obligations

5.4. Where there are reasonable grounds to suspect that an Eligible Data Breach may have occurred, Council will engage a Data Breach response as outlined in the Guideline.

Containment

5.5. Once aware of a suspected or actual Data Breach, Council's Privacy Contact Officer is to direct the Response Team or relevant staff to undertake swift action to contain the breach and minimise resulting damage.

5.6. Concurrently, the Privacy Contact Officer is to direct staff to carry out the assessments noted in clause 5.7 i.e. assess whether Council is dealing with an Eligible Data Breach.

CESSNOCK CITY COUNCIL
Integrity, Respect, Teamwork, Accountability and Excellence

Assessment

5.7. Assessment of Data Breaches must be in accordance with the Guideline and the PPIP Act, and must take in consideration any guidance provided by the NSW Privacy Commissioner. Assessors must take into consideration any factors relevant to the Data Breach including but not limited to:

5.7.1. the types of personal information involved in the breach,

5.7.2. the sensitivity of the personal information involved in the breach,

5.7.3. whether the personal information is or was protected by security measures,

5.7.4. 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,

5.7.5. the likelihood the persons specified in clause 5.7.4

i. have or had the intention of causing harm, or

ii. could or did circumvent security measures protecting the information,

5.7.6. the nature of the harm that has occurred or may occur,

5.7.7. 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.

Notification

5.8. Where a Data Breach is determined, or there are reasonable grounds for it to be an Eligible Data Breach, Council will notify the NSW Privacy Commissioner and affected individuals as per the Guideline.

5.9. Notifications are to be recorded in Council's Public Notification Register (DOC2023/192850) which is available on Council's website.

Corrective action

5.10. Any preventative efforts flagged as part of the assessment that can be implemented concurrently should be, and any post incident review that needs to be undertaken or complied with should be.

5.11. A post incident review report will be compiled (as well as any preventative efforts) based on the type and seriousness of the Data Breach within 30 days Council first held reasonable suspicion about the breach. The Privacy Contact Officer can authorise an extension outside of the 30 days if the assessment report cannot be reasonably compiled within the time however the Privacy Commissioner must be notified of this decision as required by the PPIP Act.

5.12. After the incident has been assessed and notification has taken place, the Privacy Contact Officer will identify any actions required to prevent further breaches. These actions may include recommended changes to system and physical security, recommend changes to any Council policies or procedures or revision or changes recommended to staff training and education.

6. ROLES AND RESPONSIBILITIES

Privacy Contact Officer or their nominee

6.1. The Privacy Contact Officer determines if a Data Breach has occurred and if it is an Eligible Data Breach.

6.2. The Privacy Contact Officer is responsible for ensuring notification procedures are followed and relevant people notified.

6.3. The Privacy Contact Officer is to consult system owners and gain legal advice before allowing intrusion activity to continue for the purpose of gathering further data or evidence.

6.4. Once a Data Breach has been finalised, the Privacy Contact Officer is responsible for maintaining all Data Breach documentation in accordance with record keeping requirements and practices.

6.5. The Privacy Contact Officer ensures a post-incident review report is completed.

Managers

6.6. Managers are accountable for Data Breaches relating to the information collected or handled by their teams.

6.7. Managers are responsible for ensuring that the Executive Leadership Team (**ELT**) and the IT Manager are notified and sufficiently briefed in relation to Data Breaches.

6.8. Managers have the authority to determine that further investigation or action in relation to a Data Breach is required.

IT Manager

6.9. The IT Manager is responsible for the security of information and adherence to Cyber Security protocols and procedures.

6.10. If IT Manager discovers or is informed of a Data Breach or a suspected Data Breach, it is the responsibility of the IT Manager to assess the severity of the incident and inform the Privacy Contact Officer.

6.11. The IT Manager is responsible for ensuring appropriate technical resources are available to contain and resolve Data Breaches.

Council Officials

6.12. Council Officials are to notify their manager, the Governance Team or the Privacy Contact Officer if they suspect a Data Breach has occurred. Councillors are expected to make such notifications to the General Manager.

6.13. It is the responsibility of all Council Officials to ensure information is handled in a secure manner.

6.14. Council must maintain all records relevant to administering this protocol in accordance with Council's Records Management Protocol.

Compliance, monitoring and review

6.15. Information on Data Breaches will be recorded and maintained in Council's internal Data Breach Register.

6.16. Administrative changes to this protocol, including its appendices, can be made without needing an ELT adoption or a resolution. An administrative change is amending the:

6.17. name and titles of Council Officials or dignitaries, references to other organisations or bodies; and

6.18. layout, numbering, grammar and syntax, spelling and the protocol administration part of the document.

Complaints

6.19. Individuals and third parties that are not satisfied with Council's management of Data Breaches affecting them will be required to lodge an internal review as per Council's Privacy Management Plan.

6.20. Administrative staff assess all incoming correspondence to determine the nature of the complaint/request for internal review and the appropriate Council Official to consider the matter. This assessment can occur prior to the specified addressee receiving the complaint/request for internal review unless it is clearly marked '*confidential and for the addressee only*'.

7. PROTOCOL DEFINITIONS AND ABBREVIATIONS

Council	means Cessnock City Council.
Council Official	includes Councillors, members of staff (permanent, casual or temporary), Council advisors, administrators, Council committee members, volunteers and delegates of Council.
Data Breach	An unauthorised access to, or unauthorised disclosure of, Personal Information held by Council.
Eligible Data Breach	Has the same meaning as the meaning in section 59D(1) of the PPIP Act: a) there is unauthorised access to, or unauthorised disclosure of, Personal Information held by a public sector agency 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, or b) Personal Information held by a public sector agency is lost in circumstances where— i. unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and ii. if the unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to an individual to whom the information relates.
Guideline	Means the Data Breach Guideline.
Personal Information	Has the same meaning as the definition in section 4 of the PPIP Act: 1) information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

Integrity, Respect, Teamwork, Accountability and Excellence

	2) Personal information includes such things as an individual's fingerprints, retina prints, body samples or genetic characteristics; and for the purposes of Part 6A of the PPIP Act (mandatory notification of Data Breaches), it includes (s59B) *health information* within the meaning of the *Health Records and Information Privacy Act 2002* (NSW).
PPIP Act	means *Privacy and Personal Information Protection Act 2022* (NSW).

8. PROTOCOL ADMINISTRATION

Business Group	Corporate and Community Services		
Responsible Officer	Manager IT, Privacy Contact Officer		
Author	Senior Legal and Governance Officer		
Associated Guideline	Data Breach Management Guideline - DOC2021/181598	**Is this a local policy document pursuant to Part 3, Chapter 7 of the *Local Government Act 1993* (NSW)?**	No
Protocol Review Date	10-11-2024 (Annually)		
File Number / Document Number	DOC2020/055613		

This protocol supports Council's compliance with the following legislation:

- *Privacy and Personal information Protection Act 1998* (NSW)
- *Health Records Information Protection Act 2002* (NSW)
- *Privacy Act 1988* (Cth)
- *Government Information (Public Access) Act 2009* (NSW)
- *State Records Act 1998* (NSW)
- Privacy Code of Practice for Local Government 2019 (NSW)

This protocol contributes to the achievement of the following desired outcome or objectives as per Council's Delivery Program:

Civic Leadership and Effective Governance

Objective 5.3 Making Council more responsive to the community.

Related Policies / Protocols / Procedures / Documents	▪ Records Management Policy (DOC2019/038769) ▪ Privacy Management Plan (DOC2014/005148) ▪ Cyber Security Plan (DOC2022/186755) ▪ Data Breach Management Standard Operating Procedure (**SOP**) (DOC2023/150023) ▪ IPC Guideline - Guidelines on the assessment of data breaches under Part 6A of the PPIP Act ▪ IPC Guideline - Guidelines on the exemption for risk of serious harm to health or safety under section 59W ▪ IPC Guideline - Guidelines on the exemption for compromised cyber security under section 59X

Integrity, Respect, Teamwork, Accountability and Excellence

Integrity, Respect, Teamwork, Accountability and Excellence

9. POLICY AUTHORISATIONS

No.	Authorised Function	Authorised Business Unit / Role(s)
.	Assess and manage Data Breaches	General Manager Privacy Contact Officer or their nominee
	Nominate a staff member to perform the functions of the Privacy Contact Officer as outlined in this protocol and the Guideline	General Manager Privacy Contact Officer

10. POLICY HISTORY

Revision	Date Approved / Authority	Description Of Changes
1	10 November 2023 ELTCLM64/2023	Protocol adopted, replacing the Information Security Breach Protocol

11. APPENDICES