Policy

FILE NO: **PSC2023-03231**

TITLE: **DATA BREACH POLICY**

OWNER: **GOVERNANCE SECTION MANAGER**

1. PURPOSE:

1.1 Port Stephens Council ('Council') is committed to managing personal information in accordance with relevant legislation.

1.2 This Data Breach Policy ('The Policy') sets out the processes to be followed by Council staff in the event that Council experiences a data breach or suspects that a data breach has occurred. A data breach involves the loss of, unauthorised access to, or unauthorised disclosure of, personal information.

1.3 Council needs to be prepared to act quickly in the event of a data breach (or suspected breach), and determine whether it is likely to result in serious harm and whether it constitutes as a notifiable data breach.

1.4 Adherence to this Policy will ensure that Council can contain, assess and respond to data breaches expeditiously and mitigate potential harm to the person(s) affected.

2. CONTEXT/BACKGROUND:

2.1 Part 6A of the Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act) establishes the NSW Mandatory Notification of Data Breach (MNDB) scheme.

2.2 The MNDB Scheme requires every NSW public sector agency bound by the PPIP Act to notify the Privacy Commissioner and affected individuals of eligible data breaches.

2.3 Under the scheme, Council is required to prepare and publish a Data Breach Policy (DBP) for managing such breaches.

2.4 Depending on the size and nature of a data breach, the consequences for individuals can be significant. They can give rise to a range of actual or potential harm to individuals. These consequences can include financial fraud, identity theft, damage to reputation and even violence.

2.5 Data breaches can also have serious consequences for Council. A breach may create risk through the disclosure of sensitive information, or otherwise impact an Council's reputation, finances, interests, or operations. Ultimately, data breaches can lead to a loss of trust and confidence in Council and the services we provide.

3. SCOPE:

3.1 How Council has prepared for a data breach:

a) Training and awareness

i. Most data breaches, both in Australia and internationally, involve a human element (e.g. either through direct human error or cyber-attacks that rely on a human compromise). Building a well-trained and aware workforce is a strong front-line defence against breaches and other privacy risks. Council conducts routine and targeted privacy training for all staff, technical ICT officers and the Senior Leadership Team including training endorsed by NSW Cyber Security. Current cyber threat trends are monitored by relevant staff within Council who communicate alerts to Council staff when appropriate.

ii. General privacy awareness training is provided to staff upon the commencement of employment that outline Council's obligations for identifying and managing data breaches. In addition to this, communications are relayed to staff on a periodic basis and general awareness is published on Council's website under the Data Breach Management page.

b) Processes for identifying and reporting breaches

i. Council's paramount goal is to detect data breaches quickly as to be able to better contain it and mitigate any potential harms through prompt action. Council has in place multi layered technical controls to protect data loss as well as constant monitoring services managed both in house and through a third party managed detection and response provider. Additional measures taken by Council include internal and external audits that are undertaken throughout the year that serve to identify Council's existing practices and processes reflect best practice standards and protect Council appropriately.

ii. When a data breach has been identified, Council staff will raise the breach through the incident management system. If a breach has been identified by a contractor or member of the public, they can notify Council by lodging a data breach notification through Council's website on the 'Data Breach Management' page or, alternatively, by calling Council and asking to speak with the Privacy Officer.

c) Appropriate provisions in contracts / other collaborations

i. Council is often required to outsource functions to external service providers or another agency (for example, for IT solutions). These relationships are covered by either legally binding contracts, memorandums of understanding or non-disclosure agreements. To ensure Council meet it's obligations under the PPIP Act, these agreements include provisions in relation to the management and notification of data breaches.

3.2 What constitutes an eligible data breach?

a) An 'eligible data breach' occurs where:

i. 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

ii. 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.

b) Each data breach should be assessed on a case-by-case basis but some examples of data breaches may include:

i. loss or theft of physical devices
ii. sending an email to the incorrect email address
iii. misconfiguration or over-provisioning of access to sensitive systems
iv. inadvertent disclosure
v. social engineering
vi. hacking

c) Breaches can also occur between agencies, within an agency and external to an agency.

d) The MNDB scheme applies to breaches of 'personal information' as defined in section 4 of the PPIP Act, meaning information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

e) The scheme also applies to 'health information,' defined in section 6 of the Health Records and Information Privacy Act 2002 (HRIP Act), covering personal information about an individual's physical or mental health, disability, and information connected to the provision of a health service.

f) The scheme does not apply to data breaches that do not involve personal information or health information, or to breaches that are not likely to result in serious harm to an individual. Where the scheme does not apply, Council is not required to notify individuals or the Commissioner but should still take action to respond to the breach. Council may still provide voluntary notification to individuals where appropriate.

3.3 Plan for managing data breaches

a) Contain

i. In order to ensure Council's response to data breaches is easily and quickly put into action, upon receipt of the breach notification the Response Team will conduct an initial assessment of the breach and ensure triage measures are put in effect within the first 24 hours of being made aware of the breach. The Privacy Officer will write to the Privacy Commissioner during this time to advise of the suspected breach.

b) Assess

i. The initial assessment will be in accordance with the PPIP Act and may involve liaison with relevant Council staff to ensure the breach is contained in order to minimise any possible damage. Once the breach has been contained, an assessment will be carried out by the Privacy Officer by way of reviewing all of the information involved in the breach and the risks associated with the risk to determine a plan of action and/or implement any additional actions identified to further mitigate risks. The Privacy Officer will seek to determine if the breach may likely cause serious harm to those affected.

c) Notify

i. Parties (both individuals and organisations) affected by the breach may be notified as well as the Privacy Commissioner. The method of notification to the parties will depend on what contact information Council has on file but generally this notification will occur by way of either email or a hardcopy letter.

d) Review

i. A post incident review report will then be compiled (as well as any preventative efforts) based on the type and seriousness of the breach within 30 days Council first held reasonable suspicion about the breach. The Head of the Agency 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 written to with notification of this decision.

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

3.4 Obligations including external engagement or reporting

a) In some cases, agencies will have notification obligations under both the MNDB scheme and under the Commonwealth Notifiable Data Breach (NDB) scheme.

b) For example, a data breach at a NSW public sector agency that involves Tax File Numbers and is likely to result in serious harm would be reportable to both the Office of the Australian Information Commissioner (OAIC) under the Commonwealth NDB scheme, and the NSW Privacy Commissioner under the MNDB scheme.

c) The MNDB scheme has been designed to be consistent with and adopt, as far as possible, key features of the Commonwealth NDB scheme.

d) Any agencies involved in a notifiable data breach will be relayed to the Privacy Commissioner in the Assessment Report as a key contact with their relevant role to Council identified.

3.5 Communications strategy

a) When an individual or third party organisation has been identified within the course of the Assessment period the Response Team will consider whether they need to be contacted in accordance with the PPIP Act. The key contact for these parties will be the Privacy Officer within the Response Team. Communications will be carried out in writing, if practical to do so.

3.6 Capability, expertise and resourcing

a) Council must ensure staff who make up the Response Team have the necessary expertise, training and capability of adequately addressing a breach and its impact. Council commits to ensuring this is consistently monitored to ensure access to relevant practices within the data breach space are maintained.

b) Any third party contractor that undertakes cyber incident response functions on the behalf of Council must possess the relevant industry standard qualifications and expertise required.

3.7 Roles and responsibilities

a) The Response team may comprise of staff in the following positions:

Position	Responsibilities
Head of the Agency or General Manager	Consideration of report
Governance Section Manager	Governance advice, consideration of report and assessment
Governance Coordinator	Governance advice and assessment
Legal Services Manager	Legal advice
Enterprise Risk Manager	Risk advice
ICT Maintenance and Support Coordinator	ICT advice
Communications Section Manager	Communications advice
Human Resources Manager	HR advice
Corporate Applications Coordinator	Key corporate systems advice

b) Any agency head, executive officer, privacy officer, staff member, third party contractor has a duty to report any suspected data breach. If a member of the public identifies a suspected breach they are encouraged to notify Council as soon as possible.

c) If the General Manager is involved in a suspected breach in such a way that may discount their ability to consider the report, the suspected data breach will be considered by the delegated Head of Agency.

d) If the delegated Head of Agency is involved in a suspected breach in such a way that may discount their ability to consider the report, the delegation will be revoked for the purpose of considering the suspected data breach and such data breach will be considered by the General Manager.

e) The Mayor and Councillors will notify the Head of the Agency of any data breaches they suspect may have occurred. Any data breach notifications received from the elected body will be processed by the Head of the Agency.

f) Council staff are required to raise any suspected breach via the incident management system and notify their immediate supervisor and Section Manager.

g) The Governance personnel within the Response Team will be responsible for providing advice on suspected data breaches as well as the management of any raised suspected data breaches including the assessment and notification of relevant parties. Further to this, Governance will be responsible for determining reporting obligations, liaising with the IPC & stakeholders, maintaining this policy, record keeping and conducting the post-breach review and evaluation.

h) The Response Team may also seek advice from 3rd Party privacy specialists or the NSW Information and Privacy Commission if deemed necessary as part of the assessment process.

3.8 Record Keeping

a) Council will maintain a public register in accordance with s 59O on its website that contains any notifications given under s59N(2) concerning notifiable data breaches that have occurred within the last 12 months. In addition to this public notification, an internal register for eligible data breaches will be maintained.

b) Records may also be kept in Council's electronic management system.

3.9 Post breach Review and Evaluation

a) In order to understand what went wrong, how issues were addressed and whether changes were needed to processes and procedures following a breach will mitigate future risks and are key to ensuring Council continues to proactively manage data breaches in line with the PPIP Act and community expectations.

b) Following the assessment period and finalisation of the data breach assessment report the Response Team will collaborate to ensure any weaknesses in handling data are remediated. The aim of this will be to identify what contributed or caused the breach and how to prohibit this from occurring again. Ongoing assessment of how the Response Team managed the breach will also contribute to Council's wholistic effectiveness when responding to a data breach.

4. DEFINITIONS:

4.1 An outline of the key definitions of terms included in the policy.

Assessment Period	As defined by s 59J of the PPIP Act
Head of the Agency	The General Manager or appropriately delegated staff member
IPC	Information and Privacy Commission
Public Sector Agency	As defined under section 3 of the PPIP Act. Relevantly subsection (f) includes a local government authority (Council).

Privacy Officer	Governance Section Manager or appropriately delegated staff member
Response Team	The General Manager, staff within Council's Governance Section and staff within both the ICT Maintenance and Support Unit and Corporate Applications Unit. Staff within the communications section and Human Resources section may be included in the response unit.

5. STATEMENT:

5.1 Making a Data Breach Policy publicly accessible enhances transparency and ensures agencies remain accountable for the way they respond to data breaches. It also enhances public trust and confidence in government and the services it provides.

6. RESPONSIBILITIES:

6.1 The Governance Section Manager is responsible for implementing, complying with, monitoring, evaluating, reviewing and providing advice on this policy.
6.2 Employees of Council are responsible for complying with this policy.

7. RELATED DOCUMENTS:

7.1 Privacy and Personal Information Protection Act 1998 NSW
7.2 Health Records and Information Privacy Act 2002 NSW
7.3 Privacy Act 1988 Cth
7.4 Privacy Management Plan
7.5 Code of Conduct
7.6 ICT Systems Access and Cyber Security Management Directive

CONTROLLED DOCUMENT INFORMATION:

This is a controlled document. Hardcopies of this document may not be the latest version. Before using this document, check it is the latest version; refer to Council's website: www.portstephens.nsw.gov.au.			
EDRMS container No.	PSC2023-03231	**EDRMS record No.**	23/187611
Audience			
Process owner	Governance Section Manager		
Author	Governance Section Manager		
Review timeframe	3 years	**Next review date**	12 September 2026
Adoption date	12 September 2023		

VERSION HISTORY:

Version	Date	Author	Details	Minute No.
1	12.9.23	Governance Section Manager	Original policy adopted by Council.	205