DATA BREACH POLICY

Adopted: xxxxx

Trim: xxxxxx.2024

DATA BREACH POLICY

DIRECTORATE: **Corporate Support**

BUSINESS UNIT: **Governance Legal & Procurement**

1. PURPOSE OF POLICY

1.1 The purpose of this policy is to set out how Liverpool City Council will respond to a data breach in a timely and effective manner and to ensure Council's compliance with the Mandatory Notification of Data Breach ("MNDB") Scheme.

2. AIM OF POLICY

2.1 This Policy:

- Provides guidance for responding to a breach of information held by Council.
- Provides considerations around notifying persons whose privacy may be affected by the breach.

2.2 Assists Council in avoiding or reducing possible harm to both the affected individuals and organisations and Council and may prevent future breaches.

2.3 This Policy is supplemented with more detailed internal guidance for Council staff to follow, in Council's Data Breach Response Plan.

3. SCOPE

3.1 This policy applies, wherever practicable to

(a) Councillors;
(b) Council employees;
(c) Council's consultants and contractors;
(d) Council-owned businesses; and
(e) Council committees (including community members of those committees which may be established under section 355 of the Local Government Act 1993.

4. POLICY STATEMENT

4.1 A data breach could have serious consequences for Council, creating risk through the disclosure of sensitive information which can impact the reputation, finances, interests or operations of Council.

4.2 Additionally, a data breach can damage Council's relationship with the community by creating a loss of trust and confidence in Council and the services provided.

4.3 Responding quickly in the event of a data breach can substantially reduce the impact on any affected individuals and Council. Responding to a data breach includes determining if there has been an eligible data breach which is reportable under the MNDB scheme.

5. LEGISLATIVE CONTEXT

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

5.2 The MNDB scheme requires that, in the event of an eligible data breach, Council must notify the Privacy Commissioner and affected individuals.

5.3 Section 59ZD of the PPIP Act requires Council to develop and publish a Data Breach Policy (DBP), to explain how Council will respond to any eligible data breaches. This DBP establishes the roles and responsibilities of Council staff in relation to managing a breach and outlines broadly the steps Council will follow when a breach occurs.

6. PRINCIPLES

6.1 The MNDB scheme applies to data breaches involving '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 determined from the information or opinion. The scheme also applies to 'health information' within the meaning of the Health Records and Information Privacy Act 2002 ("HRIP Act").

6.2 The MNDB scheme does not apply to:

- data breaches that do not involve personal information or health information, or to
- data breaches where it is assessed that the breach is not likely to result in serious harm to an individual.

6.3 Where the scheme does not apply, Council is not required to notify individuals or the NSW Privacy Commissioner. Council should still take action to respond to the breach and consider whether its other obligations require notification of the breach to the impacted parties or other entities that may have provided the breached data.

6.4 In some cases, Council may also be subject to the Commonwealth Notifiable Data Breach Scheme ("NDBS") which is reportable to the Office of the Australian Information Commissioner ("OAIC"). An example would be where a

data breach involves Tax File Numbers. Council's *Data Breach Response Plan* explains these rules in more detail for Council staff.

7. DEFINITIONS

Data Breach means an incident in which there has been unauthorised access to, unauthorised disclosure of, or loss of, personal information held by (or on behalf of) Council.

Data breaches can be caused or exacerbated by a variety of factors, affect different types of personal information, and give rise to a range of actual or potential harms to individuals, businesses and agencies. There is overlap between information security incidents and data breaches, but they are not exactly the same. Some cybersecurity incidents will not impact on anyone's personal information. Some data breaches will involve only hard copy information such as paper files.

Eligible Data Breach means the Unauthorised Access to, or Unauthorised Disclosure of, Personal Information held by Council where 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.

Where Personal Information held by Council is lost in circumstances where Unauthorised Access to, or Unauthorised Disclosure of, the information is likely to occur and 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.

These are reported to the Information and Privacy Commission NSW under the NSW MNDB scheme pursuant to Part 6A of the PPIP Act. .

In determining whether a breach is an eligible data breach for the purposes of the MNDB scheme, an assessment needs to be made based on the unique circumstances of the breach, the data lost and the potential that the breach may result in serious harm to the individuals to whom the data relates.

Employees means all full time, part time, casual, temporary and fixed term employees, agency staff and contractors. For the purpose of this policy, employees also include volunteers, trainees, and students on work placements.

Personal Information	means information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.
Health Information	means personal information that is information or an opinion about an individual's physical or mental health, or a disability, and information connected to the provision of a health service.
Unauthorised Access	means the access of personal and health information held by Council by a person or persons without appropriate delegation or authority to do so.

8. EXAMPLES OF A DATA BREACH

8.1 Examples of a data breach include:

(a) Cyber incident such as ransomware, malware, hacking, phishing or brute force access attempts resulting in access to or theft of data.
(b) A device with data is lost or stolen.
(c) Information is mailed or emailed to the wrong person.
(d) Hardcopy records with personal information is left in a discarded cabinet.

8.2 Not all data breaches will involve personal information, however for a data breach to be considered an eligible breach under the MNDB Scheme the breach must involve personal information.

9. RESPONSE TO A DATA BREACH

9.1 Each data breach is unique and requires a tailored response. Response actions will depend on factors such as the type of data compromised, the cause of the breach, and the potential harm that could arise for affected individuals.

9.2 While the details of each breach will be different, the process for responding to a data breach will follow the same steps. Council has developed a clearly defined process and well-defined roles and responsibilities for dealing with breaches which enables a quick and effectively response in an emergency.

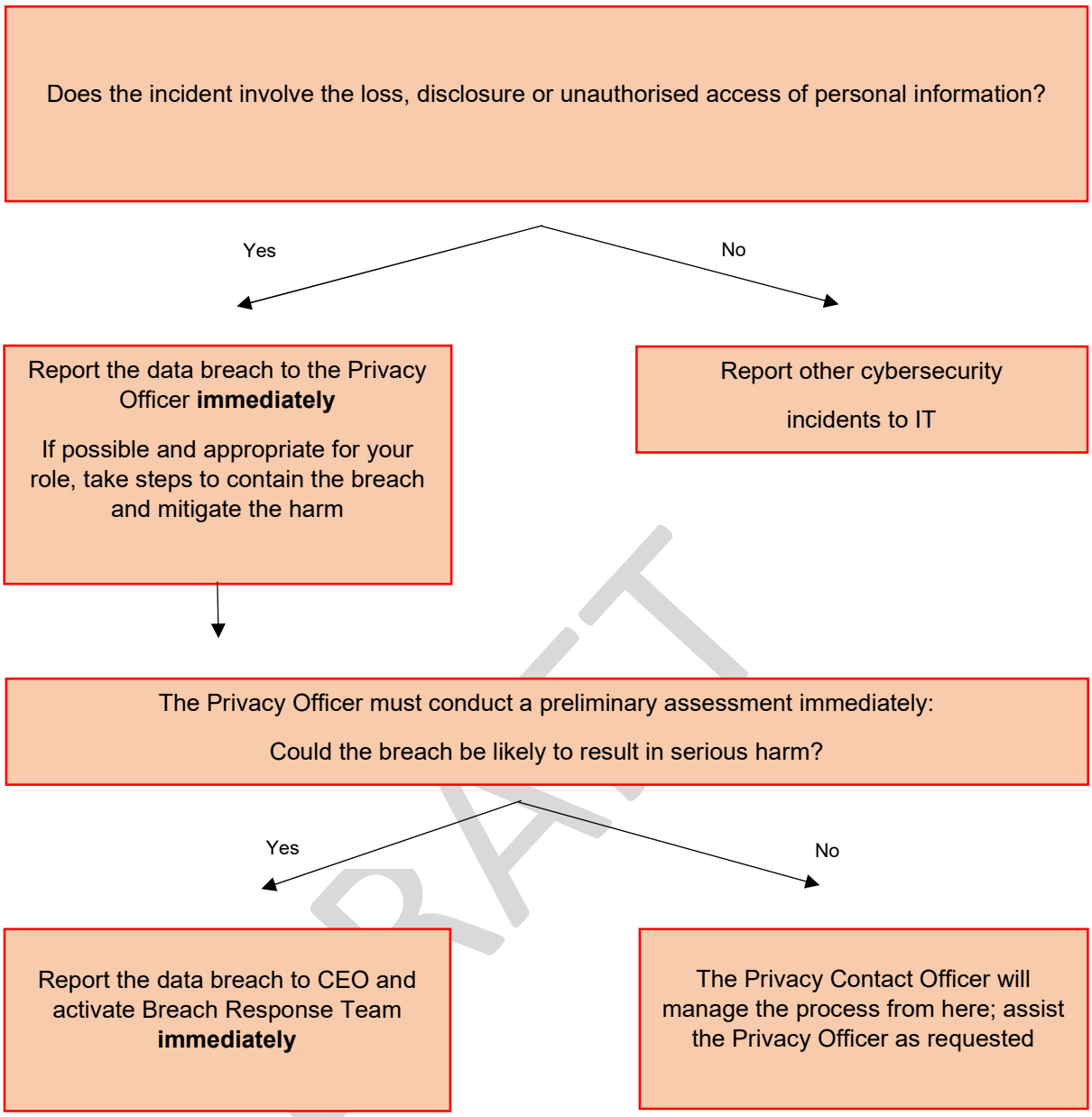
9.3 The following principles will be followed when dealing with a data breach.

(a) Initial Report and Triage
(b) Contain
(c) Assess & mitigate
(d) Notify
(e) Review
(f) Document and Record

9.4 The flow chart below illustrates the steps undertaken by staff in making a preliminary assessment of a reported Data Breach. Council's Data Breach

Response Plan explains these steps and the relevant responsibilities in more detail for Council staff.

Chart 1: Preliminary assessment of a reported Data Breach



10. APPOINTMENT OF A DATA BREACH RESPONSE TEAM

10.1 Council's Privacy Officer will be responsible for determining whether a Data Breach Response Team will be convened. Considerations may include:

(a) the type and sensitivity of information involved
(b) whether the information was protected by security measures
(c) the persons to whom the information was exposed, or
(d) the risk of harm to the individuals involved and the nature of any potential harm.
(e) the number of individuals potentially impacted by the breach
(f) any suspected external exposure of individuals' personal information
(g) any suspected unlawful activity

10.2 The Data Breach Response Team will include:

(a) Council's Privacy Officer.
(b) Council's General Counsel
(c) The team leader or coordinator of the team from where the breach originated.
(d) Manager of the section from where the breach originated.
(e) In the event of a Cyber incident, the Chief Information
(f) Where the breach involves employee data, the Manager, People & Culture
(g) Manager, Media and Communications Team
(h) Any other employee/contractor who can assist in the investigation.

10.3 The Data Breach Response team will address the specifics of any identified breach and take steps to protect the Council's data holdings and mitigate the potential harm to any impacted parties. The Data Breach Response team will be guided in their response by the Council's internal Data Breach Response Plan.

11. TRAINING AND AWARENESS

11.1 Council will ensure that its employees are aware of and understand this Policy and Council's internal Data Breach Response Plan, including how to identify and report actual or suspected data breaches. This Policy will be published on Council's intranet and website.

11.2 Various forms of communication will be used to provide regular reminders to employees of their obligations regarding personal information and health information, and how to reduce the risk of human error data breaches from occurring.

12. MEMBERS OF THE PUBLIC

12.1 Members of the public who become aware of a potential or suspected data breach involving Council information should advise Council's Privacy Contact Officer by:

Emailing: governance@liverpool.nsw.gov.au

Calling: 1300 36 2170

RELEVANT LEGISLATIVE REQUIREMENTS

Privacy and Personal Information Protection Act 1998
Health Records and Information Privacy Act 2002
Privacy Act (Cth) 1988

RELATED POLICIES & PROCEDURE REFERENCES

Liverpool City Council Privacy Policy adopted 29 April 2020
IPC Guide to Preparing a Data Breach Policy (May 2023)
IPC Guide to Managing Data Breaches in Accordance with the PPIP Act (June 2023)
IPC Data Breach Policy (October 2023)

AUTHORISED BY

Council Resolution

EFFECTIVE FROM

This date is the date the policy is adopted by Council resolution.

REVIEW DATE

The policy must be reviewed every two years or more frequently depending on its category or if legislative or policy changes occur.

VERSIONS

The current and previous version of the policy should be set out in the following table.

Version	Amended by	Changes made	Date	TRIM Number
New				

THIS POLICY HAS BEEN DEVELOPED IN CONSULTATION WITH

Governance
Legal
Information Technology
Audit Risk and Improvement

ATTACHMENTS

NIL