



Item No: 2.7
Title: For Public Exhibition - Draft Privacy Management Plan Policy and Data Breach Policy
Department: Corporate Services

12 December 2023 Ordinary Council Meeting

Reference: F2010/00542 - D15972512
Author: Alysha Croussos, Senior Governance Officer, Governance
Manager: Edward Hock, Unit Manager Governance, Risk and Legal
Executive: Marissa Racomelara, Director Corporate Services

Recommendation

That Council:

- 1** ***Places the following documents on public exhibition for a period of 28 days as per this report:***
 - ***Privacy Management Plan Policy***
 - ***Data Breach Policy***
- 2** ***Considers a further report be presented following the public exhibition period for consideration of any relevant submissions and adoption of the documents.***

Report purpose

To outline Council's obligations under the Mandatory Notification of Data Breach Scheme arising from the recent amendments to the *Privacy and Personal Information Protection Act 1998 (PIIP Act)* and seek endorsement to place the reviewed Data Breach Policy and Privacy Management Plan Policy on public exhibition.

Executive Summary

This report details the proposed changes made to the enclosed documents following recent amendments to the PPIP Act and seeks Council endorsement to seek community feedback.

Background

The recent amendments made to the PPIP Act came into effect on 28 November 2023.

The key change to the PPIP Act is the introduction of the Mandatory Notification of Data Breach Scheme (**MNDB Scheme**). The MNDB Scheme requires public sector agencies (such

2.7 For Public Exhibition - Draft Privacy Management Plan Policy and Data Breach Policy (contd)

as Council) bound by the PPIP Act to notify the Privacy Commissioner and affected individuals of **eligible data breaches** involving personal or health information that are likely to result in serious harm.

Under the MNDB Scheme, Council has an obligation to:

- Immediately make all reasonable efforts to contain a data breach and undertake an assessment **within 30 days** where there are reasonable grounds to suspect there may have been an '*eligible data breach*' (the timeframe for assessment can be extended in accordance with the PPIP Act),
- During the assessment period, make all reasonable attempts to mitigate the harm done by the suspected breach,
- Decide whether a breach is an eligible data breach or there are reasonable grounds to believe the breach is an eligible data breach,
- Notify the Privacy Commissioner and affected individuals of the eligible data breach, and
- Comply with other data management requirements as set out in the PPIP Act.

An eligible data breach occurs where:

1. There is 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**
2. A reasonable person would conclude that the access or disclosure of the information would likely to result in serious harm to an individual to whom the information relates.

The obligations set out above, in addition to other obligations imposed by amendments to the PPIP Act, require Council to ensure it has a robust data governance framework that complies with the MNDB Scheme. This includes:

- Establishing clear roles and responsibilities for managing a data breach or suspected data breach,
- Reviewing and updating Council's *Privacy Management Plan* to include provisions in relation to the procedures and practices used by Council to ensure compliance with the obligations and responsibilities set out in Part 6A of the PPIP Act. The Plan is required to reference Council's *Data Breach Policy*,
- Preparing and publishing (or in Council's case, review) a *Data Breach Policy* that sets out how Council will respond to a data breach, the roles and responsibilities of Council staff in relation to managing a data breach and the steps Council will follow if a breach occurs,
- Establishing and maintaining an internal register of data breaches, and

2.7 For Public Exhibition - Draft Privacy Management Plan Policy and Data Breach Policy (contd)

- Establishing and maintaining a public notification register of any public notifications made. The information in the public notification register must be publicly available for at least 12 months after the date of publication.

Current Status

In response to these requirements, Council has reviewed the following documents relevant to the MNDB Scheme:

- Privacy Management Plan Policy
- Data Breach Policy
- Data Breach Procedure

A summary of the changes is outlined below:

Policy Name	Changes
Privacy Management Plan Policy	<ul style="list-style-type: none"> • Transferred to Council's new Policy template as required under Council's Policy Documents Framework • Renamed to the <i>Privacy Management Plan Policy</i> to align with Council's policy Documents Framework • Confirmed that actual processes and procedures are outlined correctly within the Policy
Data Breach Policy	<ul style="list-style-type: none"> • Transferred to Council's new Policy template as required under Council's Policy Documents Framework
Data Breach Procedure	<ul style="list-style-type: none"> • Reviewed to align with the requirements of the PPIP Act and MNDB Scheme as well Council's current processes and procedures • Further information provided in terms of roles and responsibilities

While the Data Breach Procedure is not presented for public exhibition as it is operational in nature, it is provided as part of this report for consideration and context.

Consultation

Executive Leadership Team
 Governance
 Customer Service
 Information Technology
 Procurement
 Legal

2.7 For Public Exhibition - Draft Privacy Management Plan Policy and Data Breach Policy (contd)

People and Culture
Facilities and Asset Management
Communications

Financial Considerations

At its meeting held 19 October 2020, Council resolved the following:

1108/20 That any motions put before Council for the remainder of this term of Council that have financial implications require the Chief Executive Officer to provide a report on how those additional costs will be met.

The following statement is provided in response to this resolution of Council.

It is anticipated that there are limited financial impacts in adopting the proposed documents. Any new or additional training that needs to be provided to staff can be provided in-house using current resources and/or additional training materials provided free of charge by the Information and Privacy Commission (IPC) on their website.

Link to Community Strategic Plan

Theme 4: Responsible

Goal G: Good governance and great partnerships

R-G2: Engage and communicate openly and honestly with the community to build a relationship based on trust, transparency, respect and use community participation and feedback to inform decision making.

Risk Management

If Council does not align with the requirements of the MNDB Scheme, it will be in breach of the PPIP Act and may face regulatory action.



Options

1. Endorse the draft policies and place on public exhibition for community feedback and consultation. **This is the recommended option.**
2. Resolve not to endorse the draft policies and not exhibit the documents as reviewed. This is not the recommended option as the review ensures compliance with the MNDB Scheme and PPIP Act.

Critical Dates or Timeframes

The amendments to the PPIP Act and the commencement of the MNDB Scheme commenced on 28 November 2023. It is noted that Council is broadly compliant already; however, these recommended changes align with the amended legislation and the requirements of the MNDB Scheme.

Attachments

- 1** DRAFT Privacy Management Plan Policy Provided Under Separate Cover D15782319

- 2** DRAFT Data Breach Policy Provided Under Separate Cover D15871538

- 3** DRAFT Data Breach Procedure Provided Under Separate Cover D15871576
