Parliamentary Counsel's Office

Data Breach Policy

August 2026

Approved by Parliamentary Counsel 30.08.2026

Contents

Table of Contents

Policy Owner / Contact

Corporate Services

Review Record

Date	Action	Version
July 2026	Draft	1.0

1. Overview

This policy outlines the principles and requirements members of the Parliamentary Counsel's Office (PCO) must comply with when responding to personal information data breaches, including eligible data breaches under the *Privacy and Personal Information Protection Act 1998* (PPIP Act), Part 6A. PCO is required to prepare and publish a data breach policy under the PPIP Act, section 59ZD.

PCO is committed to the responsible management of the personal information it collects and holds, and to managing data breaches in accordance with the PPIP Act. Data breaches can cause harm to affected individuals, damage PCO's reputation and result in non-compliance with legal obligations.

This policy applies to all PCO employees, including ongoing, temporary and casual staff, and contractors, consultants and service providers engaged by PCO, agency staff engaged to perform work on behalf of PCO, secondees, work experience students and volunteers and any other authorised persons with access to PCO information, systems or networks (all authorised users).

This policy will be reviewed every two years, or earlier if required due to legislative, operational or organisational changes.

2. Roles and responsibilities

Role	Key responsibility
Parliamentary Counsel	Overall accountability for the management of data breaches within PCO, including ensuring compliance with PIPP Act and approving notifications to affected individuals and regulators if required.
Director, Corporate Services and Operations	Ownership and ongoing review of this policy and the Data Breach Response Plan, including coordinating responses to data breaches, assessing impacts and notification requirements, and keeping records of data breaches and response actions.
Manager, Cyber Security	Coordinating the technical response to cyber security incidents involving personal information, including investigation, containment, remediation and advice on cyber security risks and controls.
Employees, contractors and other authorised persons with access to PCO information, systems and networks	Compliance with this Policy and the Data Breach Response Plan, including protecting personal information and reporting actual or suspected data breaches as soon as practicable.

3. Policy

3.1 What is a data breach

A data breach occurs when personal information held by PCO is accessed, disclosed, used, modified or lost without authorisation.

Personal information includes information or an opinion about an identifiable individual. It also includes health information as defined in the *Health Records and Information Privacy Act 2002*.

Data breaches may result from malicious activity, human error or failures in information handling or security controls.

Examples of data breaches include:

- unauthorised access to personal information held in PCO systems, or
- phishing or malware incidents that compromise personal information, or
- loss or theft of a laptop, USB device or paper record containing personal information, or
- loss or theft of a personal device containing or providing access to PCO records or information, or
- sending personal information to an incorrect recipient, or
- accessing personal information for purposes unrelated to official duties.

A data breach may occur within PCO, between PCO and another government agency, or through unauthorised access by an external party.

3.2 Impact of data breaches

The impact of a data breach will depend on the nature of the information involved, the extent of the breach and the circumstances surrounding the breach.

A data breach may cause serious harm to affected individuals, whether the breach involves a single individual or a large number of individuals. Potential harms include:

- identity theft or fraud, or
- financial loss, and
- threats to personal safety, and
- psychological or emotional distress, and
- reputational damage, and
- embarrassment or loss of trust.

A data breach may also adversely affect PCO, including through:

- reputational damage, or
- loss of public confidence, or
- financial or operational impacts, or
- compromise of PCO information, systems, networks or services.

3.3 Reporting of data breaches

A report of a data breach or suspected data breach should be made as soon as practicable to the Director, Corporate Services and Operations or the Parliamentary Counsel.

When reporting an actual or suspected data breach, the following information, to the extent known, should be provided:

- the date and time the breach occurred or was identified,
- a description of the breach, including how the breach occurred,
- the type of information involved, including whether personal or health information is affected,
- the number of individuals potentially affected,
- any actions already taken to contain or mitigate the breach,

- whether the breach involves a cyber security incident,
- details of any third parties involved in the breach,
- any other information relevant to assessing the potential impact of the breach.

The public may report data breaches to PCO using the contact details on the PCO website.

A data breach is an eligible data breach if a reasonable person would conclude that the breach is likely to result in serious harm to an individual whose personal information is involved.

If an eligible data breach is identified, PCO must notify affected individuals and the NSW Privacy Commissioner in accordance with the PIPP Act.

All decisions regarding the assessment and notification of eligible data breaches will be made by the Director, Corporate Services and Operations or Parliamentary Counsel, in accordance with legislative requirements.

3.4 Responding to data breaches

All PCO employees, contractors and authorised users must respond promptly to actual or suspected data breaches and report the breaches to the Director, Corporate Services and Operations or the Parliamentary Counsel.

PCO's response to a data breach will generally involve:

- Containment-Taking immediate steps to contain the breach, prevent further unauthorised access, disclosure, use, modification or loss and establish the known facts of the incident.
- Assessment-Assessing the nature and extent of the breach, the information involved, and whether the breach is likely to result in serious harm to affected individuals.
- Notification-If required by law, notifying the NSW Privacy Commissioner and affected individuals. Consideration may also be given to voluntary notification if it is appropriate to do so.
- Review-Reviewing the cause of the breach, identifying lessons learned, and implementing measures to reduce the risk of similar breaches occurring in the future.

If a data breach involves a cyber security incident, the Manager, Cyber Security will coordinate the technical response and recovery activities.

4. Further information

Relevant guides and legislation:

- Privacy and Personal Information Protection Act 1998 (NSW)
- Health Records and Information Privacy Act 2002 (NSW)