



Privacy data breach and complaints procedure

Version: 1.0 | Version effective: 27/01/2026

Audience

Department-wide

Purpose

This procedure outlines the process the Department of Education (the department) and its employees must follow when responding to a privacy data breach or a privacy complaint, to comply with the [Information Privacy Act 2009 \(Qld\)](#) (IP Act) and/or [Privacy Act 1988 \(Cth\)](#).

Overview

Process A: Responding to a privacy data breach outlines how to respond to a privacy data breach, which can occur when the department fails to manage personal information in line with its obligations under the IP Act. For students, additional protections apply under section 426 of the [Education \(General Provisions\) Act 2006 \(Qld\)](#), which restricts the recording, use, or disclosure of their personal information unless specific exceptions apply.

A data breach involves unauthorised access, disclosure of information held by the department, or the loss of information held by the department where unauthorised access or disclosure is likely to occur. If the data breach involves personal information and could result in serious harm to individuals, it may be deemed an eligible data breach under section 47(1) of the IP Act. The department must notify the Queensland Office of the Information Commissioner (OIC) and affected individuals about an eligible data breach under the Mandatory Notification of Data Breaches (MNDB) scheme. The department has 30 days to assess suspected breaches from the date of forming a reasonable suspicion of a privacy data breach.

Process B: Managing a privacy complaint outlines how to manage a privacy complaint, which can arise when an individual believes their personal information has been mishandled. The department must respond within 45 business days of receiving a complaint. The complainant can refer the complaint to the OIC for mediation after 45 business days where they have either not received a response from the department, or they have received a response but are dissatisfied with the outcome.

Privacy complaints may also be [customer complaints](#), human rights complaints or Charter of Victims' Rights complaints and if applicable, must be recorded and reported as such.

Responsibilities

All employees

- understand and comply with legislative requirements for collecting, using and managing personal information, including protecting it from unauthorised access, disclosure or loss
- undertake relevant privacy training as applicable to their role
- seek guidance from their manager, principal, director or above regarding potential privacy data breaches
- report suspected privacy data breaches or complaints to their manager, principal, director or above or the Privacy team in a timely manner
- support investigations into privacy data breaches or privacy complaints as required.

Managers, principals, directors and above

- refer suspected privacy data breaches or complaints to the Privacy team for advice and support
- contain, assess and respond to privacy data breaches under the guidance of the Privacy team
- notify affected individuals if an eligible data breach is likely to have occurred
- call emergency services if a privacy data breach poses an immediate and serious risk of harm
- consider human rights when investigating and responding to a privacy data breach or privacy complaint
- consider if the [Charter of Victims' Rights](#) is engaged when investigating or responding to a privacy data breach or privacy complaint
- work with the Privacy team to manage privacy data breaches and privacy complaints within statutory timeframes
- document all assessments, actions and outcomes in an authorised recordkeeping system
- provide information to the Privacy team to support the department's eligible data breach register
- assist with implementing strategies to reduce further loss or harm from a privacy data breach or privacy complaint and prevent or minimise the risk of recurrence.

Privacy team

- maintain appropriate policies, procedures, resources and training to support employees to identify and report privacy data breaches
- lead the department's privacy data breach and complaint response activities, including assessment, coordination, and advice
- provide guidance on managing, containing, and mitigating privacy data breaches and complaints
- determine whether a breach meets the threshold for mandatory notification under the MNDB scheme or if exceptions apply
- support departmental areas to notify affected individuals and others, where required
- consider human rights when investigating and responding to a privacy data breach or privacy complaint
- consider if the [Charter of Victims' Rights](#) is engaged when investigating and responding to a privacy data breach or privacy complaint

- notify internal or external stakeholders as required and escalate within the department as appropriate
- maintain the department's eligible data breach register, reporting requirements and public notifications published to the department's website
- analyse trends in privacy data breaches and complaints to inform education and prevention strategies
- provide quarterly and annual privacy, human rights and Charter of Victims' Rights complaints reporting
- liaise with regulators and tribunals as appropriate.

Privacy Director

- notify the Office of the Information Commissioner of eligible data breaches as required under the MNDB scheme.

Complainant

- make a privacy complaint about the department's handling of their own personal information (or that of their child, in the case of a parent/carer)
- lodge the complaint within 12 months of becoming aware of the incident
- provide the complaint in writing, with sufficient detail about the incident and include contact information.

Process

Process A: Responding to a privacy data breach

Identify and report the breach

Employees must:

- immediately report suspected privacy data breaches to their manager, principal, director or above, and to the Privacy team using the [Privacy data breach form](#) (DoE employees only). Examples of privacy data breaches include:
 - losing a USB flash drive containing personal information
 - emailing personal information to the wrong recipient
 - discussing personal information acquired during your role with unauthorised person/s
 - failing to apply correct security controls to personal, sensitive or protected documents
 - accessing personal information irrelevant to your work
- provide relevant information and documents to the Privacy team for advice and to assist with assessments.

Contain and mitigate the breach

The manager, principal, director or above, in consultation with the Privacy team, must undertake an initial evaluation of the privacy data breach to inform containment and harm mitigation strategies. This will include a risk assessment as outlined in the [Enterprise risk management procedure](#), and will consider specific privacy factors such as:

- the nature and sensitivity of the information

- the amount of information involved and the number of affected individuals
- the ease of identifying individuals
- the seriousness of potential harm
- the existence of security protections and the likelihood of those being compromised
- any other mitigation measures already in place.

If a privacy data breach is likely to cause serious harm to an individual, the manager, principal, director or above must immediately contact emergency services.

The Privacy team will:

- provide advice on the application and interpretation of the IP Act
- provide referrals to or engage other departmental teams to support the privacy data breach response as necessary
- discuss and recommend reasonable actions to mitigate the breach, such as:
 - recalling an email directed to the wrong recipient
 - removing information from public domains such as the school's websites or social media accounts
 - securing information in the workplace (for example, locking computers or storing documents securely)
 - preventing further unauthorised use or disclosure of the personal information, for example, updating systems to reflect changed parent or student contact arrangements
 - suspending the activity that led to the privacy data breach.

The manager, principal, director or above, in consultation with the Privacy team, must action any containment and harm mitigation measures as quickly as possible to protect personal information and prevent any further damage or harm.

Assess the breach

The manager, principal, director or above, in consultation with the Privacy team, must comprehensively assess the severity of the privacy data breach, evaluate the risks and the likelihood that it will result in serious harm to any individual whose personal information was involved in the privacy data breach.

The department has a statutory timeframe of 30 days to assess whether there is an eligible data breach from the date of forming a reasonable suspicion of a privacy data breach. If the potential for serious harm is identified for any individual, the breach would fall under the mandatory reporting obligations of the MNDB scheme.

Examples of potential eligible data breaches include:

- losing or misplacing documents containing personal or sensitive information
- disclosing sensitive personal information to external parties
- inappropriate access by an employee to restricted internal files containing sensitive personal information
- accidentally making an online internal database or portal publicly available

- cyberattacks, phishing, malware or hacking incidents that allow external parties to access sensitive personal information.

To ensure an objective assessment, an employee not involved in the privacy data breach, but under the guidance and oversight of the Privacy team, would be most appropriate to assess the likelihood of serious harm to individuals whose personal information was involved. The employee will consider physical, psychological, emotional, financial, or reputational harm, as well as other types of harm that may meet the serious threshold. Serious harm considerations will include:

- the kind of personal information accessed, disclosed or lost
- the sensitivity of the personal information
- whether the personal information is protected by one or more security measures
- if the personal information is protected by one or more security measures – the likelihood that any of those security measures could be overcome
- the individuals, or the types of individuals, who have obtained, or who could obtain, the personal information
- the nature of the harm likely to result from the data breach
- any other relevant matter.

The [Privacy data breaches page](#) (DoE employees only) contains further resources to assist with the evaluation of privacy data breaches and the assessment of serious harm.

The manager, principal, director or above, in consultation with the Privacy team, must also determine if the privacy data breach has affected a victim of a violent crime and therefore engaged the Charter of Victims' Rights. The [Guideline: Charter of Victims' Rights Complaints](#) (DoE employees only) details how to make this assessment.

Notify about the breach

If the Privacy team reasonably believes an eligible data breach has occurred, the manager, principal, director or above must:

- provide the Privacy team with necessary information to:
 - identify all affected individuals
 - make any mandatory notifications to the OIC
 - update the department's Eligible data breach register.

The Privacy team will:

- determine if any statutory exemptions from notification requirements apply
- advise the manager, principal, director or above on:
 - mandatory notification obligations, including who must be notified, what to include and when to notify
 - voluntary notifications, where appropriate
- manage incoming inquiries from other agencies involved in the disclosure
- consult with any affected external stakeholders, contractors or other third parties.

Notify individuals

As soon as practicable, the manager, principal, director or above must notify individuals, as advised by the Privacy team. How affected individuals and other entities affected by the privacy data breach are notified will depend on the type and scale of the breach, as well as the immediate practical issues such as having contact details for the affected individuals/organisations. Notifications can be made by:

- directly contacting each individual whose personal information was involved, if possible
- contacting each affected individual, if notifying all individuals is not possible, or
- publishing a public notification on the department's website for at least 12 months, if notifying each individual or each affected individual is not practical.

If the notice is published online by the Privacy team, the Privacy team must also inform the OIC how to access the notice so the OIC can publish it on its website for at least 12 months.

The manager, principal, director or above must:

- include the following details in the notification (as far as reasonably practicable):
 - the department's name (and any other affected agency)
 - contact details for the nominated person in the department
 - the date the breach occurred
 - a description of the breach
 - how the breach occurred and what type of personal information was involved
 - the amount of time the personal information was disclosed for
 - actions that have been taken or are planned to secure the information, or to control or mitigate the harm
 - recommendations about the steps an individual should take in response to the breach
 - how individuals can make a privacy complaint
- act as key contact and manage enquiries and communications with affected individuals
- document all actions and outcomes in an authorised recordkeeping system.

Notify the Office of the Information Commissioner

The Privacy Director must provide a written statement to the Queensland OIC as soon as practicable after confirming an eligible data breach. The statement must include:

- the same information provided in the individual notification (see previous section)
- a description of the personal information involved (without disclosing specific details)
- whether the report is being made on behalf of other agencies, and the names of those agencies
- the total number (or best estimate) of individuals whose personal information was accessed, disclosed or lost and affected individuals
- the total number (or best estimate) of individuals who have been notified of the breach
- whether individuals were informed about how to make a privacy complaint.

Notify other entities

The department may need to notify other agencies or organisations, as required by law, contract or circumstances. The Privacy team will assess whether any of the following need to be notified, based on the nature and scope of the breach. For example:

- Crime and Corruption Commission Queensland - if the breach involves suspected corrupt conduct
- Queensland Police Service - if the breach involves theft or other suspected criminal activity
- Queensland State Archivist - if the breach involves loss, damage or unauthorised destruction of public records
- Queensland Government Information Security Virtual Response Team – for cyber or information security incidents that meet reporting thresholds
- Office of the Australian Information Commissioner - if the breach triggers obligations under the *Privacy Act 1988* (Cth) (for example, in relation to Tax File Numbers)
- Minister, financial service providers, professional associations, regulatory bodies or insurers, as required.

Record the breach in the Eligible data breach register

For every eligible data breach, the Privacy team must record accurate and complete information in the department's Eligible data breach register. This includes:

- a clear description of the breach, including the type of breach that occurred
- the dates when any statements or additional information were provided to the OIC
- who was notified about the breach (for example, affected individuals, internal teams, external regulators) and how they were contacted
- any exemptions relied on (if applicable)
- the steps taken to contain the breach and minimise further harm
- the actions taken to prevent similar breaches from happening in the future.

If any information is not available at the time of initial entry, the Privacy team must update the register with the missing information as soon as practicable after it becomes known.

Conduct post-incident review and remediation

To build knowledge and assist with the prevention of breaches, the Privacy team, in consultation with the manager, principal, director or above, must undertake a post-incident review, that:

- analyses all aspects of the privacy data breach
- determines the relevant causes
- identifies key learnings
- establishes short and/or long-term remedial measures. Examples may include:
 - a security audit of both physical and technical security controls
 - a review of policies and procedures

- a review of employee training practices
- a review of obligations with contracted service providers
- communication to schools, regional and central offices, student safety, and integrity and employee relations teams
- assigns responsibility for actioning and monitoring remediation activities.

The manager, principal, director or above will ensure the privacy data breach and remedial measures are accurately recorded in an authorised recordkeeping system.

Process B: Managing a privacy complaint

Receive and report the complaint

A privacy complaint can be made by:

- an individual about how the department has handled their own personal information, or
- a parent/carer on behalf of a student.

The complainant must:

- submit the complaint in writing to a departmental employee
- include an address for the department to respond to
- provide details of the incident that is the subject of the complaint
- lodge the complaint within 12 months of becoming aware of the incident.

The employee who receives the complaint, through their manager, principal, director or above, must:

- report the complaint to the Privacy team at privacy@qed.qld.gov.au
- ensure the complaint is recorded in a register, such as the Customer Complaints Management System (CCMS), in line with the [Customer complaints management procedure](#)
- consider relevant human rights under the [Human Rights Act 2019 \(Qld\)](#) (for example, Section 25 privacy and reputation) and whether the [Charter of Victims' Rights](#) is engaged.

Acknowledge and assess the complaint

The Privacy team will:

- contact the complainant (or their authorised representative) in writing to:
 - clarify the details of the complaint and the outcomes they are seeking
 - explain the complaints process and set expectations
- assess whether the complaint relates to a breach of the [Information Privacy Act 2009 \(Qld\)](#) (IP Act) or the [Privacy Act 1988 \(Cth\)](#) (where applicable). If the complaint does not relate to a breach of privacy legislation, the Privacy team will:
 - notify the complainant (or their authorised representative) in writing that their issue is not assessed as a privacy complaint

- provide information on how to lodge a customer complaint unrelated to privacy concerns
- record the decision to close the complaint and document the actions taken. No further action is required under this procedure
- determine if the complaint involves an eligible data breach (see Assess the breach), and if so, follow the MNDB scheme requirements as outlined in the Notify about the breach section.
- identify if the complaint falls within multiple complaint frameworks and refer any non-privacy related components to the appropriate team (that is, school, regional office, legal services or integrity and employee relations).

Investigate the complaint

The Privacy team will:

- investigate the facts and circumstances of the complaint
- engage with the relevant school, region or business unit to gather necessary documents and speak with individuals directly involved in the incident
- provide advice to the manager, principal, director or above on the application and interpretation of the [IP Act](#)
- determine the extent to which the complaint can be partially substantiated, fully substantiated or is unable to be substantiated, by:
 - confirming the complaint relates to the complainant's (or their child's) personal information, and the level of personal information involved
 - validating the cause of the complaint, for example, a data breach resulting from human error, cyber breach, inadvertent publication or incorrect email recipient
 - assessing the complaint against the department's obligations under the IP Act and associated Queensland Privacy Principles (QPPs)
- if the complaint is substantiated, determine appropriate actions to resolve it. These may include:
 - employee training
 - process changes
 - technology system reconfiguration
- report any instances where human rights have been limited under the [Human Rights Act 2019 \(Qld\)](#) (based on the assessment completed in the Receive and report the complaint section)
- report if the [Charter of Victims' Rights](#) is engaged (for example if the complainant is a victim of violent crime)
- assist with public inquiries relating to complaints that arise from a privacy data breach.

The manager, principal, director or above must work with the Privacy team to take the necessary actions to resolve the complaint and prevent similar breaches in the future.

The Privacy team and manager, principal, director or above must keep written records of all interactions with the complainant (or their authorised representative) during the investigation, including diary notes of phone

calls or meetings. These records are essential if the complaint cannot be resolved and escalates to mediation or legal proceedings through the Office of the Information Commissioner (OIC) and/or the Queensland Civil and Administrative Tribunal (QCAT).

The [Records management page](#) (DoE employees only) provides further information about how to make, manage and dispose of records.

Respond to the complaint

The Privacy team, in consultation with the manager, principal, director or above, must:

- respond to the complainant (or their authorised representative) within 45 business days
- provide a written outcome letter that clearly explains the department's decision and includes:
 - a summary of the context and nature of the complaint
 - an assessment of the complaint against relevant privacy principles and obligations
 - any other relevant information considered in the assessment
 - actions the department will take to comply with the MNBD scheme, if an eligible data breach has occurred
 - advice that the complainant may refer the complaint to the OIC for mediation if they are not satisfied with the outcome.
- respond in accordance with the Charter of Victims' Rights if the charter has been engaged
- record the correspondence, actions taken and outcome in the applicable authorised recordkeeping system or complaints register.

Refer the complaint to the Office of the Information Commissioner

The complainant may refer the complaint to the OIC for mediation if 45 business days have passed and they have either not received a response from the department or are dissatisfied with the outcome of the response.

The Privacy team must:

- support the mediation process between the department and the complainant. This may involve:
 - providing a submission, including relevant arguments or representations, to help the OIC determine whether to accept the complaint
 - working with relevant business units, schools or regional offices to participate in the mediation. Mediation discussions may cover:
 - the merits of the complaint
 - the complainant's preferred outcome
 - any concerns or issues that may prevent agreement on the proposed outcome
 - negotiations with the complainant about their response to the proposed resolution
- record the outcome of any mediation in the appropriate departmental register.

If the complaint cannot be resolved through OIC mediation, the OIC will provide the complainant with the option to refer the complaint to QCAT for further review.

Definitions

Term	Definition
Affected individual	A person whose personal information is involved in a privacy data breach and who is likely to suffer serious harm as a result.
Authorised recordkeeping system	<p>An ICT business system designed to capture, manage and provide access to records through time, that is intended to preserve the context, authenticity and integrity of the records. Authorisation is provided by a principal, an executive director or above, ensuring compliance with recordkeeping requirements such as Public Records Act 2023 (Qld) and Queensland Government Records governance policy. Examples of approved recordkeeping systems include Content Manager for regional and central offices, the OneSchool (DoE employees only) suite of applications for schools or suitable secure file location on school servers.</p> <p>ICT business systems that do not qualify as an authorised recordkeeping system include email systems (such as Outlook), OneDrive, Teams.</p> <p>Further information can be found in OnePortal under Records management (DoE employees only) and Information asset and recordkeeping procedure.</p>
Customer complaint	<p>A customer complaint is defined within section 264(4) of the Public Sector Act 2022 (Qld) as a complaint about the service or action of a department, or its staff, by a person who is apparently directly affected by the service or action. Examples may include complaints about:</p> <ul style="list-style-type: none"> • a decision made, or failure to make a decision, by a departmental employee • an act, or failure to act, by the department • the formulation of a proposal or intention by the department • the making of a recommendation by the department • the customer service provided by a departmental employee. <p>Refer to the Customer complaints management procedure for further information.</p>
Data breach	<p>A 'data breach' extends to any information held by the department and refers to:</p> <ul style="list-style-type: none"> • unauthorised access to, or unauthorised disclosure of, the information • the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of the information is likely to occur.

Term	Definition
Eligible data breach	<p>An 'eligible data breach' only involves personal information. For a data breach to be an 'eligible data breach' triggering notification and other obligations under the Mandatory Notification of Data Breach scheme, both of the following must apply:</p> <ul style="list-style-type: none"> • there is unauthorised access to, or unauthorised disclosure of, personal information held by the department, or there is a loss of personal information held by the department in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur • the unauthorised access to, or disclosure of the information is likely to result in serious harm to an individual to whom the personal information relates (an 'affected individual').
Employee	<p>Any permanent, temporary, seconded, casual or contracted staff member, contractors and consultants or other person who provides services on a paid basis to the department that are required to comply with the department's policies and procedures. Within schools this includes principals, deputy principals, heads of department, heads of curriculums, guidance officers, teachers and other school staff. Volunteers depending on the engagement may not be considered employees but should have regard for this procedure.</p>
Personal information	<p>Information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion:</p> <ul style="list-style-type: none"> • whether the information or opinion is true or not, and • whether the information or opinion is recorded in a material form or not.
Privacy complaint	<p>A privacy complaint is a complaint by an individual about an act or practice of the department or an employee in relation to the individual's personal information that is, or may be, a breach of the department's obligations under the <i>Information Privacy Act 2009</i> (Qld) and associated Queensland Privacy Principles.</p>
Privacy data breach	<p>A privacy data breach or potential breach may include an action or omission that results in loss, theft, misuse or unauthorised disclosure or use of personal information. A privacy data breach occurs if the department does not deal with a person's personal information in accordance with its obligations under the <i>Information Privacy Act 2009</i> (Qld) and associated Queensland Privacy Principles</p>
Queensland Privacy Principles (QPPs)	<p>Rules under Schedule 3 of the <i>Information Privacy Act 2009</i> (Qld) that govern how personal information is collected, stored, used, and disclosed. There are 10 principles the department must adhere to.</p>
Sensitive information	<p>Sensitive information includes:</p> <ul style="list-style-type: none"> • information or an opinion about an individual's: <ul style="list-style-type: none"> ○ racial or ethnic origin

Term	Definition
	<ul style="list-style-type: none"> ○ political opinions ○ membership of a political association ○ religious beliefs or affiliations ○ philosophical beliefs ○ membership of a professional or trade association ○ membership of a trade union ○ sexual orientation or practices ○ criminal records ● health information about an individual, or ● genetic information about an individual that is not otherwise health information, or ● biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or ● biometric templates.
Serious harm	Harm to an individual caused by unauthorised access or disclosure of their personal information. This could include serious physical, psychological, emotional, financial, or reputational harm.

Legislation

- [Crime and Corruption Act 2001 \(Qld\)](#)
- [Education \(General Provisions\) Act 2006 \(Qld\)](#)
- [Human Rights Act 2019 \(Qld\)](#)
- [Information Privacy Act 2009 \(Qld\)](#)
- [Privacy Act 1988 \(Cth\)](#)
- [Public Sector Act 2022 \(Qld\)](#)
- [Public Records Act 2023 \(Qld\)](#)
- [Right to Information Act 2009 \(Qld\)](#)
- [Victims' Commissioner and Sexual Violence Review Board Act 2024 \(Qld\)](#) Chapter 3, parts 3-4
- [Child Safe Organisations Act 2024 \(Qld\)](#)

Delegations/Authorisations

- [Delegation of Director-General's powers under Education \(General Provisions\) Act 2006](#)

Policies and procedures in this group

- [Information management, privacy and security policy](#)
- [Administrative access to information procedure](#)
- [Copyright procedure](#)
- [Information asset and recordkeeping procedure](#)

Supporting information for this procedure

- Nil

Other resources

- [A guide to the Charter of Victims' Rights](#)
- [Code of conduct for the Queensland public service](#)
- [Customer complaints management procedure](#)
- [Education futures institute catalogue](#) (DoE employees only)
- [Guideline: Charter of Victims' Rights Complaints](#) (DoE employees only)
- [Human rights](#) (DoE employees only)
- [Information Privacy Principles](#)
- [Information privacy course](#) (DoE employees only)
- [Obtaining and managing student and individual consent procedure](#)
- [Privacy's OnePortal site](#) (DoE employees only)
- [Privacy data breaches](#) (DoE employees only)
- [Queensland Office of the Information Commissioner: Privacy data breach management and notification](#)
- [Records management OnePortal page](#) (DoE employees only)
- [Use of ICT systems procedure](#)

Contact

For further information about privacy, please contact:

Privacy team, Privacy and Safer Technologies

Email: privacy@qed.qld.gov.au

For further information on ICT policies, procedures and standards, please contact:

Governance, Risk and Compliance Unit

Email: ictpolicy@qed.qld.gov.au

Review date

27/01/2029

Superseded versions

Previous seven years shown. Minor version updates not included.

2.0 Information privacy breach and privacy complaints procedure

Creative Commons licence

Attribution CC BY

Refer to the [Creative Commons Australia](https://creativecommons.org/) site for further information