Procedure

Information privacy breach and privacy complaints procedure

Version: 2.0 | **Version effective**: 15/04/2024

Audience

Department-wide

Purpose

This procedure outlines the process the Department of Education (the department) and its employees must follow in response to a privacy breach or a privacy complaint.

Overview

The department is committed to maintaining public confidence by managing breaches of personal information and associated complaints in a timely and fair manner. This procedure outlines the steps required by the department and its employees to ensure the reporting and management of privacy breaches or privacy complaints relating to an individual's personal information is accountable, compliant, transparent and timely.

A **privacy breach** occurs when the department (represented by their employees) has not managed an individual's personal information in a manner consistent with its obligations under the *Information Privacy Act 2009* (Qld). Student personal information is also further protected by section 426 of the *Education (General Provisions) Act 2006* (Qld) and cannot be recorded, used or disclosed unless one of the exceptions in section 426 applies.

Privacy breaches can result from technical issues, human error, inadequate procedures and training, a misunderstanding of the law, or deliberate acts. Common causes of a breach include human error, the loss, theft, or unauthorised collection, access, use, or disclosure of personal information (for example, a USB flash drive is lost, or an email is sent to unintended recipients).

A **privacy complaint** occurs when an individual notifies the department that they believe their personal information has not been managed in a manner consistent with the department's obligations under the *Information Privacy Act 2009* (Qld), associated information privacy principles or other relevant legislation. A privacy complaint may arise as a result of a privacy breach.

Privacy complaints that are also customer complaints or human rights complaints must be recorded and included in departmental reporting. Privacy complaints have a statutory timeframe of 45 days in which the department must respond. If the department fails to respond to the complainant within the statutory 45-day period, the

complainant may refer their privacy complaint directly to the Office of the Information Commissioner (OIC), Queensland.

Responsibilities

All employees

- be aware and understand their obligations to comply with legislative requirements for the collection, use and management of personal information and the department's code of conduct by completing annual training as applicable to their role:
  - Mandatory All-Staff Training (MAST) program (DoE employees only)
  - Management Foundations program (DoE employees only).
- seek advice from their manager, principal, director or above for guidance to determine if a privacy breach has occurred
- report any privacy breaches or complaints to their manager, principal, director or above in a timely manner
- action any requests for information by employees who are investigating privacy breaches or privacy complaints.

Managers, principals, directors and above

- seek advice from the department's Privacy and Safer Technologies unit (Privacy team) for guidance to determine if a privacy breach has occurred and how to respond to ensure compliance with the department's statutory privacy obligations
- refer any suspected privacy breaches or complaints, and all supporting documents to the department's Privacy team
- assess whether there is any potential for harm to any individual or the department and where necessary take steps to manage and mitigate such harm (refer to Privacy breaches (DoE employees only) for information)
- review and manage privacy breaches and privacy complaints referred to the school or business unit, after assessment by the Privacy team
- ensure their employees action any requests for information by the persons investigating the privacy breach or privacy complaint in a timely manner, noting the department must respond within statutory timeframes
- document all investigations and outcomes in an authorised recordkeeping system
- assist as necessary with the implementation of strategies developed to mitigate further loss or harm as a result of a privacy breach or privacy complaint.

Privacy and Safer Technologies (Privacy team)

- provide advice and guidance to employees involved in privacy breaches or privacy complaints regarding the management, containment, assessment, response and mitigation to privacy breaches and privacy complaints
- in conjunction with other relevant business units, coordinate all privacy breach and privacy complaint response activities across the department

- assess, consider, and where necessary comply with the department's mandatory data/privacy breach notification obligations
- report privacy breaches and privacy complaints to the appropriate regulator on behalf of the department as necessary
- provide a report as necessary to the school, business unit, or regional office identifying the causes of the privacy breach or privacy complaint and suggested mitigation or training activities to prevent recurrence
- develop and provide advice regarding the implementation of the Privacy breach report
- identify trends and key themes contributing to privacy breaches and privacy complaints and incorporate these into education, training and awareness programs.

Complainant

- provide the privacy complaint in writing to a departmental employee.

Managing a privacy breach

Where possible, the first three steps of the process to manage a privacy breach should be undertaken concurrently.

1. Contain the breach

If a privacy breach has occurred, employees must act to contain the breach as quickly as possible to prevent further compromise of personal information and minimise resulting or potential damage or harm. This may include, but is not limited to actions such as:

- recalling an email directed to the wrong recipient
- removing information from the public domain such as the department's website or social media account
- securing information in the workplace by minimising, closing or putting away information (or locking the computer)
- escalating breaches internally to their manager, principal, director or above
- taking steps to prevent further unauthorised use or disclosure of the personal information for example, updating OneSchool to capture changed parent or student contact arrangements.

The manager, principal, director or above must also report the breach to the department's Privacy team, determine the source of the breach and prevent further damage or harm for example, by:

- identifying and shutting down the system or account that has been breached
- suspending the activity that led to the privacy breach
- revoking or changing access codes or passwords (refer to the identity and access management section of the Use of ICT systems procedure for guidance).

To support containment of the breach, the Privacy team will:

- provide advice on the application and interpretation of the *Information Privacy Act 2009* (Qld)
- provide assistance and guidance as necessary.

2. Evaluate the risks associated with the breach

The manager, principal, director or above must evaluate the risks and potential for harm associated with the breach in consultation with the Privacy team. Considerations include:

- Who is affected by the breach?
- What is the potential for harm to the individual, or reputational risk to the department?
- What is the foreseeable harm to the affected individuals?
- What type of personal information is involved?
- Whether the department has consent to take the appropriate action from the student's parent or the individual whose personal information is involved?
- What was the cause of the breach?
- What steps have been taken as part Step 1: Contain the breach?

Further information to assist with evaluation can be found on the Privacy breaches page (DoE employees only).

3. Respond to the breach

The manager, principal, director or above, in consultation with the Privacy team, must determine if notification of affected individuals or a parent/guardian is required. Considerations may include:

- the risk of harm and type of harm to the affected individual(s). This will involve the manager, principal, director or above considering all information they have regarding the personal circumstances of any individual for example, known violence, student protection issues, domestic violence order
- steps the department has taken to date to avoid or remedy any actual or potential harm
- if any other business units or agencies should be notified
- the ability of the individual to take further steps to avoid potential harm or remedy harm
- whether the information that has been compromised is sensitive, or likely to cause humiliation or embarrassment for the affected individual(s)
- if there is any applicable legislative provisions or contractual obligations that requires the department to notify affected individuals or other entities (for example a Memorandum of Understanding (MOU) with another Queensland Government agency)
- if the actions taken have minimised or mitigated any identified risk
- liaise with Integrity and Employee Relations unit to ensure the privacy breach is not part of an existing investigation. If the breach forms part of an existing assessment or investigation it is to be managed in consultation with Integrity and Employee Relations.

If it has been determined that notification of affected individuals is required, the principal, director or above must notify relevant individuals at risk of harm as a matter of priority.

If a risk of harm to an individual has been identified, the Privacy team must determine, depending on the severity of the breach, if it is appropriate to inform other business units of the department and/or relevant third parties for assessment or to provide support. This may include:

- Regional Principal Advisor, Student Protection
- Strategic Communication and Engagement unit
- Legal Services unit
- Intake and Assessment team within Integrity and Employee Relations
- Crime and Corruption Commission Liaison Officer within Integrity and Employee Relations
- Director-General and/or Ministerial and Executive Services unit
- any relevant third parties or regulatory bodies such as the OIC, the Office of the Australian Information Commissioner (OAIC), Child Safety, Queensland Police Service, the Queensland State Archivist or applicable online service provider.

4. Prevent a repeat of the breach

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

- If the breach is not part of an existing investigation, investigate the circumstances of the breach to determine relevant causes and identify and implement short and/or long-term measures to prevent a reoccurrence. The preventative actions may include the need for:
  - 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
  - referral of remedial actions to the manager, principal, director or above to prevent a repeat of the breach
  - where appropriate, provide a Privacy breach report to the schools, regional and central offices, and Intake and Assessment team, Integrity and Employee Relations to evaluate and document how the breach was managed for recordkeeping, the findings, and possible safety implications and for audit trail purposes.
- Store the Privacy breach report in an authorised recordkeeping system.

The manager, principal, director or above will review the Privacy breach report and its recommendations and implement any required privacy breach mitigations to prevent a recurrence.

Managing a privacy complaint

1. Acknowledge any complaints received relating to a privacy breach

Upon receipt of a privacy complaint, employees through their manager, principal, director or above must:

- report the privacy complaint to the Privacy team via email to privacy@qed.qld.gov.au
- facilitate the recording of the complaint in a register, such as the department's Customer Complaints Management System (CCMS)

- assess the complaint against human rights. This includes but is not limited to the right to privacy and reputation. For more information, refer to the summary of human rights in the context of education (DoE employees only).

The Privacy team must acknowledge the complaint either in writing or verbally to the complainant. The Privacy team may:

- explain the steps in the complaint process and expected timeframes for handling the complaint
- provide information about how the department collects, uses and discloses personal information in the course of handling a complaint
- advise a contact telephone number, preferably with the name of a contact person, from the schools, regional and central offices within the department that will be handling the complaint.

As part of acknowledging a privacy complaint, the Privacy team will assess, and where possible, resolve the privacy complaint in conjunction with the schools, regional and central offices. The Privacy team will:

- clarify the complaint, the outcomes sought, the complaint process and any expectations with the complainant or their authorised representative in writing, by telephone or in person
- decide if the issue relates to a breach of the department's obligations under the *Information Privacy Act 2009* (Qld) or if applicable the *Privacy Act 1988* (Cth)
- assess the facts and circumstances involved in the complaint, and where appropriate:
    - investigate and respond to the complainant or their authorised representative on behalf of the department
    - refer the privacy complaint back to the schools, regional and central offices for management with assistance from the Privacy team.

Should the Privacy team determine that the complaint does not relate to a breach of the relevant privacy legislation, the Privacy team must:

- advise the complainant or their authorised representative in writing that the complaint has not been assessed as a privacy complaint
- outline the options to submit a customer complaint not related to a privacy breach or concern
- record the decision to close the complaint and the actions taken.

Once such complaints are closed, the remainder of this procedure does not need to be followed and no further action is required under this procedure.

2. Investigate privacy complaints

To investigate the complaint, the Privacy team will consult with the manager, principal, director or above to:

- 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, their child, or authorised representative, the client'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 *Information Privacy Act 2009 (Qld)* and associated Information Privacy Principles (IPPs).

- Determine the actions required to resolve the complaint, this may include but is not limited to:
  - employee training
  - business process change
  - system reconfiguration.
- During the investigation, the Privacy team will:
  - provide advice to the manager, principal, director or above on the application and interpretation of the *Information Privacy Act 2009* (Qld)
  - report any instances where human rights have been limited (based on the assessment completed as part of Step 1: Acknowledging any complaints received relation to a privacy breach) in the CCMS
  - assist in responding to public inquiries about managing any complaints that may result from a privacy breach.

The manager, principal, director or above must facilitate the implementation of necessary actions to resolve the complaint in collaboration with the Privacy team and address any ongoing potential for future privacy breaches.

During the investigation, the Privacy team and the manager, principal, director or above must record (DoE employees only) any dealings with the complainant or their authorised representative in writing, for example diary notes of any conversation. If the complaint cannot be resolved and escalates, the formal record will assist the department in responding to any subsequent dealings with the complainant, their authorised representative, the Office of the Information Commissioner and/or the Queensland Civil and Administrative Tribunal (QCAT).

3. Respond to the complaint

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

- Respond to the complainant, or assist the school or business unit to respond to the complainant or their authorised representative, within 45 business days and communicate the outcome of the complaint in writing. The complaint outcome letter must provide clear reasons for the department's decision regarding the privacy complaint and, at a minimum, should demonstrate that the department has:
  - addressed the context, nature and extent of the complaint
  - assessed the complaint against the relevant privacy principles and obligations
  - considered all other relevant criteria, such as legislation applicable to the department, and any relevant policies, standards or directives
  - advised the complainant of their right to refer the complaint to the Office of the Information Commissioner for mediation if they are not satisfied with the response.
- Record the actions taken in the applicable register such as the CCMS.

4. Referral to the Office of the Information Commissioner

The complainant may refer the complaint to the OIC for mediation after 45 business days or due to dissatisfaction with the outcome. The Privacy team must assist the OIC to mediate between the department and the complainant.

Assisting the OIC may include:

- Providing a submission and/or arguments or representations on whether the OIC should accept the complaint.
- In conjunction with other relevant business units, engaging in mediations which may consider:
  - the merits of the complaint
  - the complainant's proposed outcome
  - concerns that may affect agreement on the proposed outcome
  - negotiation with both parties (the complainant and the department) in terms of their response to the proposed outcome.
- Recording the outcome of any investigations.

If the complaint cannot be resolved through the OIC, the OIC will provide the complainant with an option to refer the privacy complaint to QCAT or alternately the complainant may refer the matter to QCAT themselves.

Definitions

Term	Definition
Authorised recordkeeping system	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 2002* (Qld) and Queensland Government Records governance policy. Examples of approved recordkeeping systems (DoE employees only) include Content Manager for regional and central offices, the OneSchool (DoE employees only) suite of applications for schools. ICT business systems that do not qualify as an authorised recordkeeping system include email systems (such as Outlook), OneDrive, Teams, network drives. Further information can be found in the Records management manual (DoE employees only).
Customer complaint	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 public sector entity, or its employee, by a person who is apparently directly affected by the service or action. Examples may include complaints about: • a decision made, or failure to make a decision, by a public sector employee

Term	Definition
	• an act, or failure to act, of the public sector entity • the formulation of a proposal or intention of the public sector entity • the making of a recommendation by the public sector entity • the customer service provided by a public sector employee of the public sector entity. Refer to the Customer complaints management procedure for further information.
Employee	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, head 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.
Human rights complaint	A complainant can make a human rights complaint if the department has: • acted or made a decision in a way that is not compatible with human rights • failed to give proper consideration to a relevant human right when making a decision.
Information Privacy Principles (IPPs)	Schedule 3 of the *Information Privacy Act 2009* (Qld) contains eleven Information Privacy Principles (IPPs) which must be adhered to when dealing with personal information. The Information Privacy Principles (IPPs) place strict obligations on the department when it collects, stores, uses and discloses personal information. In summary the eleven information privacy principles relate to: • IPP 1. Lawful and fair collection of personal information • IPP 2. Collection of personal information when requested from an individual • IPP 3. Collection of personal information - ensuring relevance, completeness and currency • IPP 4. Storage and security of personal information • IPP 5. Providing information about documents containing personal information • IPP 6. Access to documents containing personal information • IPP 7. Amendment of documents containing personal information • IPP 8. Checking of accuracy, completeness and currency of personal information before use • IPP 9. Using personal information only for relevant purpose • IPP 10. Limits on use of personal information

Term	Definition
	• IPP 11. Limits on disclosure of personal information.
Personal information	Information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can be reasonably ascertained, from the information or opinion. Examples include name, contact details, medical information and financial information. Refer to the Privacy's OnePortal site (DoE employees only) for further information.
Privacy breach	A breach or potential breach may include an action or omission that results in loss, theft, misuse or unauthorised disclosure or use of personal information, or has the potential to do so. A privacy breach occurs if the department does not deal with a person's personal information in accordance with its obligations under the *Information Privacy Act 2009* (Qld) and associated Information Privacy Principles.
Privacy breach report	A report prepared as necessary by the Privacy team within Privacy and Safer technologies at the conclusion of the management of a privacy breach. The report will indicate the practices and circumstances that led to the privacy breach, the subsequent management and mitigation strategies undertaken, and proposed strategies to prevent a recurrence. The report is provided to the school or business unit where the breach occurred, and the appropriate Regional or Corporate Office with oversight of the business unit or school.
Privacy complaint	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 *Information Privacy Act 2009* (Qld) and associated Information Privacy Principles.

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)

Delegations/Authorisations

- Nil

Policies and procedures in this group

- Access to records held in schools procedure
- Copyright and other intellectual property procedure
- Information asset and recordkeeping procedure

Supporting information for this procedure

- Nil

Other resources

- Code of conduct for the Queensland public service
- Customer complaints management procedure
- Education futures institute catalogue (DoE employees only)
- Human rights (DoE employees only)
- Information Privacy Principles
- Keys to managing information (DoE employees only)
- Privacy's Oneportal site (DoE employees only)
- Privacy breaches (DoE employees only)
- Queensland Office of the Information Commissioner: Privacy breach management and notification
- Records management (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

15/04/2027

Superseded versions

Previous seven years shown. Minor version updates not included.

Creative Commons licence