



Whole of Department

Title: Information Privacy Breach Response Plan

1 Purpose and scope

The Department of Families, Seniors, Disability Services and Child Safety (the department) has obligations under the *Information Privacy Act 2009* (IP Act) to protect personal information in its possession and control. The purpose of this Privacy Breach Response Plan is to set out the procedure to be followed by departmental staff if a privacy breach, or suspected breach, occurs.

Note: Where a privacy breach arises because of an **information security incident** (e.g. denial of service, malware, ransomware, unauthorised access, use or disclosure) this plan must be read in conjunction with the Information Security Incident Response Plan.

Note: The department outsources some functions to **contracted service providers** (CSPs) to perform departmental functions. If the CSP will deal with personal information on behalf of the department, the department must take reasonable steps to bind them to comply with the IP Act. If a privacy breach is the result of the actions of a bound CSP, the CSP will be responsible for the breach response (see the Obligations of CSPs [factsheet](#)), with oversight by departmental contract managers in consultation with the Information Privacy (IP) team. If the CSP is not bound to comply with the IP Act, the department may be liable for the privacy breach.

2 Effective date

This Privacy Breach Response Plan (plan) is effective from the date of approval.

3 Application

This plan applies to all employees and contractors engaged by the department. It should be read in conjunction with other related policies, including:

- the Information Security Incident Response Plan, and
- the Business Continuity Plans for relevant areas.

Note: Officers with responsibilities under this plan and related procedures must retain them in hard copy, so they are accessible even if departmental ICT systems are affected by a cyber incident.

4 Key concepts

4.1 What is personal information?

Personal information is defined in section 12 of the IP Act as *information or an opinion, including information or 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 reasonably be ascertained, from the information or opinion.*

The department holds sensitive personal information about clients and staff, including:

- name, address, phone number, email address
- date and place of birth, race, ethnicity, religion

- medical information
- child protection information
- criminal history
- financial details
- employment information (including disciplinary information).

Note: Personal information may reveal a person’s identity even if their name is not mentioned.

Note: If there is a security incident but no personal information is involved, this plan will not apply. Refer to the Information Security Incident Response Plan.

4.2 What is a privacy breach and how do you identify one?

An **information security event** is defined as ‘an identified occurrence of a system, service or network state indicating a possible breach of information security, policy or failure of controls, or a previously unknown situation that may be security relevant’ [ISO/IEC 27000:2018].

- An **information security near miss** occurs when actions by a threat actor do not compromise confidentiality, integrity or availability, for example, attempts to do so were prevented due to security controls.

An **information security incident** is defined as ‘a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security’ [ISO/IEC 27000:2018].

- An **information security false positive** occurs when a response is triggered but further investigation determines that there was no incident.

A **data breach** occurs when *data* (which may include personal information) is shared, disclosed, or accessed without authorisation, or is lost. It may occur as the result of an information security incident (e.g. due to technical issues such as a misconfiguration or over-provisioning of access to sensitive systems, social engineering or hacking), and it may affect a large number of individuals.

An **eligible data breach** is a data breach that occurs in relation to *personal information* held by the department if:

- it involves unauthorised access to, or unauthorised disclosure of, personal information and it is likely to result in serious harm to an individual (affected person) to whom the information relates; or
- the information is lost in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur and would be likely to result in serious harm to the affected person.

A **privacy breach** occurs if the department does not handle *personal information* in accordance with its obligations under the IP Act (which may be broader than unauthorised access or disclosure). Privacy breaches can occur as a result of human error, staff misconduct, malicious activity by an external party (e.g. a cyber-attack), or unauthorised physical access to the office or files. A privacy breach may also be an eligible data breach.

Note: A *data breach* is not a privacy breach if it does not affect personal information. A *privacy breach* may occur if an information security incident affects personal information but may occur in other ways.

Examples of privacy breaches:

Human error

- Personal information is mistakenly posted or emailed to the wrong person



- Paper records containing personal information are not disposed of securely and are left in garbage or old filing cabinets
- Computer hard drives or storage devices containing personal information are disposed of without erasing the contents

Employee misconduct

- Employees access third party personal information without a work-related need to do so
- Employees send identifying information about a client to their personal email account, or to someone who does not have a legitimate 'need to know' (e.g. family or friend)
- Employees upload work documents to third party servers (e.g. to check their grammar and language) leading to privacy concerns about storage, misuse and potential overseas transfer of personal information.

Malicious activity by external party

- A database containing personal information is hacked into or otherwise illegally accessed, e.g. by:
 - Malware attack e.g. Trojan horses (programs that appear as a typical file but that hide malicious behaviour) or Ransomware (malware viruses that block access to data until a 'ransom' is paid)
 - Password attack, where a hacker guesses a password to gain access to a computer system
 - Denial-of-Service (DoS) attack, which attempts to knock a network or service offline by flooding it with traffic to the point the network or service can't cope
 - Distributed-Denial-of-Service (DDoS) attack, which hijacks devices (often using botnets) to send traffic from multiple sources to take down a network
 - Man-in-the-Middle attack, where a hacker attacks the server by sneaking through an established connection or stealing a customer's IP address and disguising themselves as the customer

Physical access to office or files

- Agency office premises are broken into, and physical files are stolen.

Sometimes, the department will become aware of a privacy breach because an anomaly is identified in an access or email audit, or because of a complaint.

Privacy breaches may also be identified by departmental employees. All employees should be aware of their privacy and confidentiality obligations and advise their line manager about any:


- errors (e.g. email sent to wrong address)
- concerns about how personal information is being handled by other employees
- concerns about processes which may not adequately protect personal information, or
- evidence of a possible security incident (e.g. phishing email).

4.3 Consequences of a privacy breach

Privacy breaches may have very serious negative impacts for affected people.

For example, unauthorised disclosure of:

- driver licence or identity documents may lead to identity theft, financial loss and psychological harm
- financial information may lead to unauthorised credit card transactions and credit fraud
- the address of a domestic violence victim may lead to intimidation or physical harm
- criminal history details may cause embarrassment, humiliation, and damage to the person's reputation
- health information may cause embarrassment and humiliation
- work disciplinary information may adversely impact a person's current or future employment.



If the privacy breach is the result of misconduct or corrupt conduct by a departmental employee, the matter will be referred to Professional Standards and may result in disciplinary action and referral to the Crime and Corruption Commission (CCC) and Queensland Police Service (QPS).

Eligible data breaches may also adversely affect the department's reputation and damage the trust clients have in the department's ability to manage their personal information. The department may also be liable to pay compensation to affected persons.

5 Procedure – key steps in privacy breach response

Privacy breaches are dealt with on a case-by-case basis, but action must be taken as soon as possible to:

- Step 1: Contain the breach
- Step 2: Identify and evaluate the risks
- Step 3: Consider whether to notify affected persons
- Step 4: Take steps to prevent future breaches.

Note: Some of these steps will be undertaken concurrently or in quick succession. The department may need to reassess the actions taken and amend its response as more information comes to hand, having regard to what remedial action can be taken to reduce any potential harm to individuals.

5.1 Incident assessment and breach containment

5.1.1 Identify the privacy breach

When a possible privacy breach is identified, you must immediately:

- discontinue any process that may be the cause of the privacy breach, and
- report it to your line manager

Note: A suspected privacy breach by a director or member of the Executive may be reported directly to the Information Privacy team.


5.1.2 Initial assessment

The responsible manager must coordinate immediate containment action and notify the Information Privacy team as soon as possible (e.g. within 1 hour of becoming aware of the breach). They must also ensure that the Privacy breaches checklist is completed and emailed to the Information Privacy team at privacy@dcssds.qld.gov.au as soon as possible.

The initial assessment must be undertaken by a person with sufficient authority (generally manager or higher) in consultation with the Information Privacy team. The manager should also notify their director about what has occurred and the proposed response. These steps should be taken within the first two hours of being made aware of the breach.

It is necessary to gather and evaluate as much information about the incident as possible. However, care must be taken to ensure that:

- evidence is not destroyed
- current or future investigations are not prejudiced, and
- the privacy principles are not breached as part of the response or any subsequent actions.



Matters to be considered as part of the initial assessment include:

- when the suspected breach occurred (if known) and when it was discovered
- the type of personal information involved
- the cause and extent of the breach
- the number and type of individuals affected, including any vulnerabilities they may have
- the nature of the possible harm, and the likelihood of harm occurring, and
- the effectiveness of possible remediation action.

These matters are considered in more detail as part of the risk assessment (see paragraph 5.2).

The Information Privacy team can provide advice and guidance, including about who else may need to be notified as part of the initial response. Notification is also discussed at paragraph 5.3.

5.1.3 Contain the breach

Where possible, immediate common-sense steps must be taken to contain the breach.

For example:

Unauthorised disclosure of personal information to a third party

- Recall emails sent to a wrong address, if possible; otherwise, ask the email recipient/s to delete the email from their Inbox and Recycle Bin/Trash and confirm when they have done so.
- Arrange to collect any mail sent or delivered to an incorrect address.
- Ask recipients not to use or disclose the information; consider whether to advise them about any applicable confidentiality obligations and the possible consequences of breaching those obligations.

Loss of device or physical files


- Recover the device or records (e.g. retrieve records left at a client's home).
- Arrange to have the mobile device remotely disabled or wiped remotely.
- Arrange a search of the site where the loss occurred (e.g. by contacting public transport, airline).
- Notify the police, if appropriate.

Data breach involving electronic records on ICT system

- Isolate the causes of the breach in the relevant system, software or database.
- Shut down the system that was breached and change computer access codes.
- Reset log-in details and passwords for compromised devices, systems or databases.
- Quarantine any compromised devices.
- Instruct employees to immediately cease a particular practice.

If the recipient is subject to confidentiality obligations (e.g. under *Child Protection Act 1999*, *Adoption Act 2009*, *Disability Services Act 2006* or the Code of Conduct) and refuses to return documents or there are concerns that they might disseminate the information, consider whether it is appropriate to remind the recipient of their confidentiality obligations.

If the person refuses to return the information, consult Legal Services. Depending on the sensitivity of the information, consider asking the police to retrieve it.



As far as possible, ensure that the recipient has not made copies, or that all copies are recovered. Depending on the circumstances, consider whether to ask the third party to complete a statutory declaration attesting that they have returned, deleted or destroyed the information and any copies.

In response to a serious security incident, it may be appropriate to engage external forensic advisors, seek external legal advice and consult IDCARE (a national identity and cyber support service). Refer to the Information Security Incident Response Plan for guidance.

5.2 Evaluate the risks

Once sufficient information is available, a risk assessment must be undertaken by the Security Incident Response Team, or the person coordinating the breach response. Relevant considerations include the extent and nature of the risk, and the likelihood of it occurring. Consider:

- *What happened?*
 - What was the date, time, duration and location of the breach?
 - Has a departmental system been compromised?
 - What was the cause and extent of the breach?

For example: Is it the result of a security incident? If so, follow the Information Security Incident Response Plan in addition to this plan.

- *What personal information was involved?*
 - How sensitive is it? Does the type of information affect the risk of harm?

For example: Unauthorised disclosure of child protection, criminal history, medical, disability or financial information, or identity documents, may create a greater risk of harm than disclosure of a person's name on a newsletter subscription list.

 - Who has been affected, noting that certain people may be at particular risk of harm?

For example: if the address of a victim of domestic violence is disclosed to the perpetrator, the risk is greater than if the recipient is a public servant who does not know the person and is subject to the Code of Conduct.

 - How many people are affected?

- *What is the context: who is affected and what is the risk of harm?*
 - Who has obtained the information?


For example: Does the recipient have a relationship with the affected person? Was the information accessed by a hacker who may publish the information or who is demanding payment of money to prevent them publishing it?

 - What is the nature of the harm likely to result from the breach?

For example: Is there a risk of physical, financial or emotional harm, reputational damage, or embarrassment?

- *What is the likelihood of the anticipated harm occurring?*
 - Has the breach been contained or mitigated?

For example: If effective containment action has been taken, the likelihood of harm occurring may be Unlikely. However, if the perpetrator has a history of publishing information on the Dark Web and has issued a ransom demand, it may be Likely.



Note: Assess the risk rating with reference to the risk assessment table in the [ICT Risk matrix | For government | Queensland Government](#)

- *Is it an ongoing breach or is there a risk of it reoccurring?*
 - Is the information protected by any security measures? Can they be overcome?
 - Has effective containment action been possible?
 - Does the breach expose a systemic issue, which means it could be repeated?

For example: Is the information on a stolen laptop or mobile phone which is password protected and its contents can be remotely wiped?

- *What is the reputational risk to the department?*

5.3 Who should be notified?

Depending on the seriousness of the breach, it may be necessary to notify internal stakeholders, external entities and affected persons. This assessment is made on a case-by-case basis.

5.3.1 Internal and external notifications

Information security breaches

As outlined above, **Information Services** must be notified immediately if the matter relates to a security incident. This is done by contacting Service Desk (ph 1300 353 574).

Manager, Information Services will brief the **Director, Information Security and Cloud Operations** about the incident.

Director, Information Security and Cloud Operations will brief the **Chief Information Officer** (CIO) and the CIO will decide whether to:

- brief the Director-General, Deputy Director-General or other senior executives
- convene the Information Security Incident Response Team (ISIRT)
- engage external forensic advisors
- notify relevant government regulators and other external bodies, including as required under the [QGEA Information security incident reporting standard](#).

Corrupt conduct or serious misconduct

Director, Professional Standards must be notified if the incident raises possible corrupt conduct or serious misconduct. They will assess the matter and, as appropriate, refer it to CCC and QPS.

Tax file numbers

A Tax File Number (TFN) breach occurs if TFN information is lost, or subject to an unauthorised access or disclosure (e.g. if a database containing TFN information is hacked; TFN records are stolen; or a TFN is provided to the wrong person). The federal [Notifiable Data Breaches scheme](#) applies to TFN breaches.

Chief Human Resources Officer must notify the Office of the Australian Information Commissioner if the breach is 'likely to result in serious harm' to an individual.



Breaches involving My Health Records

The *My Health Records Act 2012 (Cth)* (MHR Act) requires registered portal operators to report a notifiable data breach arising from their local records as soon as practicable. Breaches must be reported to the MHR System Operator (the Australian Digital Health Agency). Further information about the notification under the MHR Act is available on the OAIC's [website](#).

Manager, Data Management Services is responsible for downloading audit reports from the Australian Digital Health Agency portal and providing them to the Chief Practitioner, and **Chief Practitioner** (or their delegate) is responsible for reviewing the reports to identify any unauthorised access, and notifying the MHR System Operator, as required.

Breaches involving records of another agency/entity

If a privacy breach involves records provided by another agency, the person managing the breach response must consider whether that agency should be notified, in consultation with the IP team.

Office of the Information Commissioner

Director, RTI, Privacy, Records Management and Redress, will consider whether to notify the Office of the Information Commissioner (OIC) about a privacy breach, and notify, if required.

Litigation and insurance claims

General Counsel must be consulted if the matter raises complex legal issues or potential legal liability. General Counsel will assess whether to seek external legal advice (e.g. if the incident is serious and likely to expose the department to a class action for damages) and whether to notify the Queensland Government Insurance Fund.

Communications and media

Media Manager, Strategic Communication and Media, may need to be notified to coordinate response messaging, or if the matter is likely to result in reputational damage to the department.

Contracts and procurement


If the breach relates to the actions of a contracted service provider (CSP), the relevant Director (e.g. **Director, Family Support and Commissioning Practice, Director, ICT Procurement, Director, Property and Procurement Services**) should consider, in consultation with the IP team:

- whether the CSP has been contractually bound to comply with the IP Act
- how the department should be involved in the breach response
- how to ensure consistency in the departmental and CSP response
- what information the department can share with the CSP about the outcome of any investigation and legal advice obtained by the department
- whether the contractual arrangement should continue, be amended, or be terminated, having regard to the ability of the CSP to meet its privacy and security obligations.

5.3.2 Affected individuals

Although the IP Act does not currently require agencies to notify affected individuals, notification must always be considered. Notification is an accountability mechanism, and it can potentially mitigate the harm resulting from a breach. Failure to notify may compound the damage for affected persons and impact negatively on the department's reputation.

If a privacy breach is likely to result in serious harm to the affected person, they should be notified. Because the department will not always know the person's circumstances and the extent of the



risk, it will generally take a cautious approach and notify, to enable individuals to assess the risk of harm and take appropriate precautions.

However, if notification may cause more harm than it would alleviate (e.g., containment action has been taken and there is nothing the affected person could do to avoid or remedy the harm and notification may cause unnecessary stress and anxiety), notification may not be advisable.

The decision about whether to notify must be made by an appropriately senior person in consultation with the IP team and Legal Services, as appropriate, and the reasons documented.

For example: A decision to notify a victim of domestic and family violence that her location information has been disclosed may be made by the Manager of the relevant Child Safety Service Centre.

Each matter must be considered on a case-by-case basis. In making the assessment about notification, the matters considered in the risk assessment will be relevant, including:

- What sort of personal information has been affected?
- What are the circumstances of the breach, including its cause and extent?
- What is the risk of harm, loss, or damage to the affected person? For example:
 - Does the breach put an individual at risk of physical harm, stalking or harassment?
 - Is there a reasonable risk of identity theft or fraud? Consider the types of information lost, and whether that information together creates a risk.
 - Is the information sensitive, or likely to cause humiliation, embarrassment, or damage to the individual's reputation?
- Consider the seriousness of the harm, the likelihood of it occurring, and the ability of the individual to avoid or mitigate possible harm.
- Would notification enable the affected person to take steps to avoid, reduce or remedy harm?
- Is there a likelihood that being notified might cause the affected individual more distress than it would alleviate, particularly if there is little risk of harm?
- Are there legal/contractual obligations requiring the department to notify affected individuals?
- Are there any public interest arguments for or against notifying affected individuals?

It may be appropriate to seek independent legal advice about whether to notify affected persons.

For example: when notification should occur


- An affidavit which includes the mother's new address is served on her former partner who is the perpetrator of severe domestic violence against her.
- The department accidentally sends a copy of Disability Worker Screening card applicant's criminal history to another applicant, and the recipient is threatening to go to the media.

For example: when notification could occur

- An employee inadvertently leaves a list of employees who have enrolled to attend a training course in a cafe. The affected individuals are readily identifiable, but the potential for harm is very low.

For example: when notification need not occur

- A departmental officer loses a laptop containing personal information. The laptop is quickly recovered, and an examination by IT shows that the information has not been accessed.



- An email is sent to another public servant, but the recipient does not know the affected person and has confirmed that they have deleted the email from their Inbox and Deleted items.

5.3.4 When to notify, how to notify and who should notify

If it is assessed that affected persons should be notified, a communication plan may be useful to ensure that timely, accurate and consistent information is provided. Consider the following:

When to notify

If the affected person can take preventative action, it is important to notify as soon as possible. However, if there is no immediate action that can be taken by the affected person and the situation is rapidly evolving, it may be better to wait until the facts are confirmed, to avoid 'drip feeding' information or sharing information which is later found to be incorrect.

If the department's Professional Standards Unit, law enforcement authorities, or the CCC are involved, check with them about when to notify, so that any investigation is not compromised. However, if there is any risk to the safety of an individual, notification **must** be prioritised.

If there are many affected persons, it may be appropriate to develop a staged notification process which prioritises the people at greatest risk. For example:

- clients who had identity documents or numbers in the system
- current or active clients
- previous clients.

How to notify

Direct notification to the affected individuals (e.g. by phone, email or in person), is the preferred method because the affected persons can be notified quickly and can take any necessary action. However, in some circumstances, this might increase the risk of harm. Consider whether notification should occur in the presence of a support person (e.g. family member, counsellor, psychologist), and whether any other safeguards should be put in place to minimise the risk.

Indirect notification (e.g. posting information on the department's website, advertisements in the media) should only occur if direct notification could cause further harm, is prohibitive in cost or the contact information for affected individuals is not known and cannot reasonably be obtained. Using multiple methods of notification may be appropriate in some cases, but again you should consider whether the method of notification might increase the risk of harm to an affected individual.

Document any decisions about notification and the reasons, including assessments of risk and any safeguard measures which are implemented.



Who should notify

Generally, the area of the department that has a direct relationship with the affected individuals should be responsible for notification. However, depending on the seriousness of the breach, it may be appropriate for a more senior officer to notify the affected persons.

Consideration should also be given to what resourcing is required if a large number of people have to be notified. For example, it may be appropriate to stand up a team to manage notifications, and to prepare draft notification letters and a script for responding to queries from affected persons. In addition, the department must take steps to respond to complaints arising from the incident.

Note: If the breach is committed by a CSP which has been contractually bound to comply with the IP Act, the CSP is responsible for notification but the department may assist (see [fact sheet](#)).

What information should the notification include?

The content of the notification will vary according to the circumstances, but should include:

- the name of the agency (and any other agency/entity affected by the breach)
- the contact details of the agency (or nominated contact person)
- the date the breach occurred
- period during which access was available or disclosure was made
- a description of what occurred and how it occurred (if known)
- a description of the type of information affected (do not include any personal information)
- the steps the agency has taken or will take to contain the breach and mitigate harm
- recommendations about the steps individuals should take to mitigate harm
- an apology and information about any support the agency can provide, and
- information about how the individual may make a privacy complaint to the agency.

Note: To avoid further unauthorised disclosure, do not include unnecessary personal information, or third party personal information that is not already known to the affected persons.

For example: If information about a person who is not a party to court proceedings is included in court documents in error, and a decision is made to notify them, care should be taken when deciding what to include in the notification, because the fact that there are court proceedings may itself be confidential.

5.4 Preventing future breaches

Once the department has taken action to contain the breach, it has an obligation to identify and take steps to prevent a similar breach from occurring in the future.

Steps to identify the causes of the breach and how to prevent a recurrence may include:

- undertaking a security audit of physical and technical security controls
- mapping information flows to identify potential weaknesses
- reviewing policies and procedures to ensure they adequately address information privacy and security.

Recommendations to prevent a recurrence may include:

- implementing stronger physical and technical controls
- implementing changed work processes and updating policies/procedures
- notifying staff about any changed processes, or reminding staff about existing obligations and processes which are designed to protect personal information

- ensuring that employees involved in the incident have completed mandatory information privacy, information security, code of conduct and ethical decision-making training
- moving the employee involved in the incident to another role for a specified period
- additional oversight or supervision of staff.

5.5 Recordkeeping, reporting and review

5.5.1 Recordkeeping

All actions taken in response to the breach must be documented by the person taking the action (e.g. file noted and saved in accordance with recordkeeping obligations), so that there is evidence of how it has been managed, including breaches which are not escalated to ISIRT or the OIC.

For example: Records relevant to the Information Security incident response will be stored in accordance with the Information Security Incident Response Plan.

Records relevant to the Information Privacy breach response will be stored in Resolve.

5.5.2 Review response process

The department must also review the incident **response process** to identify any improvements for future breach responses, including any necessary or recommended amendments to this procedure or the Information Security Incident Response Plan. The review should include time frames for the implementation of any recommendations.

Depending on the nature of the breach, the review may be undertaken by the Information Security or Information Privacy team, or jointly, and overseen by the Deputy Director-General. Senior management must be briefed on the outcome of the breach response, including recommendations.

5.5.3 Identify trends and issues

The IP team will include details of the breach and response in the Information Privacy Breach Report. The IP team will review the Information Privacy Breach Report at least quarterly (or in response to serious incidents), to identify any risks, trends or systemic issues identified (e.g. type and severity of breaches, and effectiveness of response methods).

Manager, Information Privacy and Governance will report to Director, RTI, Privacy, Records Management and Redress, at least quarterly (or in response to serious incidents), on risks arising from breaches, including any trends and systemic issues.

Director, RTI, Privacy, Records Management and Redress, will brief General Counsel and Deputy Director-General/Chief Information Officer about any trends and systemic issues, as required.

5.5.4 Review Privacy Breach Response Plan

The IP team will review and update this plan annually (or in response to incidents), to ensure that it is comprehensive and up to date, and relevant staff understand their roles and responsibilities.

6 Roles and responsibilities

Director-General is responsible for ensuring that the department complies with its obligations under the *Information Privacy Act 2009* and that it takes appropriate steps in response to any privacy breaches that occur.



Deputy Director-General/Chief Information Officer is responsible for:

- ensuring that this policy is regularly reviewed and updated, is readily accessible and is communicated to all employees (and where relevant, other parties)
- overseeing Information Privacy awareness-raising through publications and campaigns
- ensuring appropriate security controls to protect information held by the department
- overseeing security incident and major privacy breach responses and the implementation of any recommendations.

Chief Practitioner is responsible for:

- ensuring that My Health Record (MHR) data which is accessed via the MHR portal is kept secure and protected from unauthorised access, use and disclosure
- overseeing audit and other review processes, and
- reporting any notifiable data breach arising from the department's local records to the MHR System Operator as soon as practicable after becoming aware of the breach.

General Counsel is responsible for notifying QGIF if there is a formal demand for compensation.

Regional Directors and Directors are responsible for:

- ensuring that TFNs are kept securely and protected from unauthorised access, use and disclosure, and assessing whether to notify the OAIC about breaches affecting TFNs
- ensuring that potential privacy breaches relating to TFNs are referred to the Information Privacy team for advice about whether the OAIC should be notified
- ensuring that alleged misconduct is assessed and responded to appropriately, including referral to Professional Standards, and through Professional Standards the CCC, and/or QPS, and appropriate action is taken.

Director, Information Policy, Security and Engagement is responsible for:

- conducting threat and risk assessments on the department's information systems
- monitoring the use of information systems and reporting any trends or security issues to the Deputy Director-General and Chief Information Officer and other relevant stakeholders
- overseeing development of Information Security training and monitoring completion rates
- overseeing the department's information security incident response, including deciding when to escalate the matter to the Information Security Incident Response team.

Director, RTI, Privacy, Records Management and Redress is responsible for:

- overseeing development of Information Privacy training and monitoring completion rates
- implementing this Privacy Breach Response Plan, including deciding when to brief senior executives about privacy breaches and any trends or systemic issues which are identified.

All managers are responsible for ensuring that:

- their teams have completed the mandatory online Information Privacy and Information Security training modules on induction and every two years
- their teams have read, understood, and acknowledged their responsibilities as outlined in this plan, including the obligation to refer privacy/data breaches to their manager
- any matters which are escalated to them are forwarded as soon as possible to the Information Privacy team and Service Desk/Information Security, as appropriate.

All employees are responsible for ensuring that:

- their Information Privacy and Information Security training (including refresher) is up to date
- they comply with Code of Conduct and legislative privacy and confidentiality obligations
- they immediately report any privacy breaches or security incidents to their manager.



7 Contact us

For more information about responding to suspected privacy breaches, contact the Information Privacy team on (07) 3097 5609 or privacy@dcssds.qld.gov.au.

For more information about responding to suspected security incidents, contact the Information Security team on (07) 3097 5705 or ISInformationSecurity@cyjma.qld.gov.au.

Date of approval: August 2024
Date of operation: August 2024
Date to be reviewed: June 2025

Office: RTI, Privacy, Records Management and Redress Branch
Help Contact: Information Privacy and Governance
Ph: (07) 3097 5609
Email: privacy@dcssds.qld.gov.au

Links

[Information Privacy Act 2009](#)

[Department of Child Safety, Seniors and Disability Services Privacy Guide](#)

[Queensland Government Enterprise Architecture Information Security Policy \(IS18:2018\)](#)

[Queensland Government Enterprise Architecture Information Security Incident Reporting Standard](#)

[Office of the Information Commissioner Privacy Breach Management and Notification](#)

[Australian Cyber Security Centre Data Spill Management Guide](#)

Deidre Mulkerin
Director-General

Appendix 1: Key contacts/stakeholders

| Contact | When to contact |
|--|---|
| Office of the Information Commissioner | If the department wishes to voluntarily report a privacy breach in accordance with the OIC's voluntary reporting scheme . Note: A Mandatory Data Breach Notification Scheme will commence on or about 1 July 2025. |
| Crime and Corruption Commission | If the breach involves corrupt conduct within the meaning of the <i>Crime and Corruption Act 2001</i> . Phone: 07 3360 6285 (Executive Director, Integrity Services) https://www.ccc.qld.gov.au/public-sector/assessing-and-notifying |
| Office of the Australian Information Commissioner | If the breach involves Tax File Numbers (TFN) or if any obligations under the <i>Privacy Act 1988</i> (Cth) apply. https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme https://www.oaic.gov.au/privacy-law/privacy-act/tax-file-numbers https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach/ |
| My Health Records System Operator (Australian Digital Health Agency) | If the breach is a contravention of the <i>My Health Records Act 2012</i> (Cth) (e.g. unauthorised collection, use or disclosure of health information included in a healthcare recipient's My Health Record, or an event occurs or circumstance arises that may compromise the MHR system: s75 MHR Act) the department must notify the System Operator in accordance with their guidelines . Contact us Australian Digital Health Agency |
| Queensland Police | Privacy breaches that involve theft or other criminal activity, e.g. computer hacking and misuse (s408E Criminal Code). QPS also has links and assistance to report cybercrime . |
| Queensland Government Insurance Fund (QGIF) | Any incident resulting in injury or financial loss where there is a formal demand for compensation from a third party should be reported to QGIF as soon as practically possible. Contact us - Queensland Government Insurance Fund (QGIF) |
| Queensland Government Cyber Security Unit | Refer to Information Security Incident Response Plan. |