Information privacy complaints and breaches procedure

Right to Information and Privacy Group

Contents

Purpose

The *Information privacy complaints and breaches procedure* (this procedure) has been developed to ensure consistency in investigating privacy breaches and complaints (privacy matters) by relevant officers of Queensland Corrective Services (QCS). It is a guide for the procedures involved in the assessment, investigation and management of privacy matters made under the *Information Privacy Act 2009* (IP Act). This procedure is to be read in conjunction with *Information privacy complaints and breaches policy*.

Roles and responsibilities

All privacy matters will be assessed, investigated and managed by the relevant officer to determine if there has been a breach of any of the 11 Information Privacy Principles (IPPs) in Schedule 3 of the IP Act. The table below sets out the relevant officers from the Right to Information (RTI) and Privacy Group involved in investigating and managing privacy matters.

Term	Definition/explanation
Receiving officer	The officer who receives the privacy matter records the information in the Client Management System (CMS) and refers the file, both electronic and hardcopy to the assessing officer. This officer may also be the assessing officer.
Assessing officer	The officer who assesses whether a privacy matter is valid and determines the classification level of the issue using the *Information privacy complaint and breach assessment triage form* (triage form). Notifies the QCS Cyber Security Unit if a suspected cyber incident has occurred.
Approving officer	The officer who approves the classification of a privacy matter on the triage form. The officer is the decision maker on a privacy matter. This may be the manager or a senior officer of the RTI and Privacy Group.
Investigating officer	The investigating officer will usually conduct the investigation in accordance with their position responsibilities and may also be the receiving officer or the assessing officer.

Privacy breach

Privacy breach is not defined in the IP Act, however, the Office of the Information Commissioner's (OIC's) website, states:

> *A privacy breach occurs when there is a failure to comply with one or more of the privacy principles set out in the Information Privacy Act 2009. Privacy breaches can occur because of a technical problem, human error, inadequate policies and training, a misunderstanding of the law, or a deliberate act. Some of the more common privacy breaches happen when personal information is lost, stolen or mistakenly disclosed (for example, a USB flash drive is lost or an email is sent to unintended recipients).*

Privacy complaint

Section 164(1) of the IP Act defines a 'privacy complaint'. The following list contains elements of the definition of 'privacy complaint' as outlined in the IP Act:

- a complaint;
- by an individual;
- about an act or practice by a relevant entity;
- in relation to the individual's own personal information; and
- that the relevant entity breached its obligations under the IP Act to comply with –
    a) the privacy principles; or
    b) an approval under section 157 (waiving or modifying the agency's obligation to comply with the privacy principles).

All privacy complaints must be sent or referred to the RTI and Privacy Group:

Email: privacy@corrections.qld.gov.au

Post: Privacy Unit, Right to Information and Privacy Group
Queensland Corrective Services
GPO Box 1054
Brisbane Qld 4001

All written or verbal privacy complaints or breaches (including self-reported breaches) must be sent or referred to the RTI and Privacy Group immediately upon receipt of the complaint.

Generally, a privacy complaint must be made within 12 months after the complainant became aware of QCS's act or practice. Complaints made outside this time period may be reviewed depending on the circumstances and merits of the matter. A privacy breach assessment report will be completed and provided as necessary to relevant management. Privacy breaches stemming from suspected cyber security incidents must be notified to the QCS Cyber Security Unit Immediately.

Individuals who complain about matters other than privacy will be referred to the *Client Complaint Management Policy*, *Individual Grievances People Capability Policy* or the *Public Interest Disclosure Policy* where relevant and advised to contact the appropriate work unit to handle their complaint.

Assistance and accessibility when making a complaint

Where an individual makes a complaint about an alleged breach of privacy and is unable to put that complaint in writing, the officer accepting the complaint must provide the individual with assistance to make their complaint in writing. This may include transcribing the individual's complaint on their behalf. The officer transcribing the complaint must read the complaint back to the individual to ensure that all of the information is captured correctly and send a copy of the complaint to the complainant.

If an individual has difficulty in making the complaint themselves, they may be supported by another person to make their complaint.

If an individual is from a culturally and/or linguistically diverse background, and requires a translator or interpreter, the Translating and Interpreter Service (TIS) may be used. The phone number for TIS is 131 450.

Where verbal assistance is provided to an individual to enable them to make a complaint, the individual must be made aware of the following privacy notice in accordance with IPP 2 of the IP Act:

> *Queensland Corrective Services is collecting your personal information from you to manage your complaint in accordance with the Privacy complaints and breaches procedure. Your personal information will not otherwise be used and disclosed unless authorised or required under a law. We will manage your personal information in accordance with the Information Privacy Principles of the Information Privacy Act 2009.*

Creating a complaint or breach file

When a privacy matter notification is received:

1. Create a file in CMS.
2. Send an eDocs number request to RecordsCentralOffice@Corrections.qld.gov.au.
3. Create the triage form and save it into the relevant file folder.
4. Enter the details into the Privacy workload register.

Comprehensive records must be kept to demonstrate that privacy matters are appropriately assessed, investigated and resolved. All correspondence including internal correspondence, reports and memoranda is to be filed and saved within the complaint file.

Quarantine access to the file to ensure QCS officers involved in the handling of the personal information which is the subject of the matter cannot access any documentation in the file.

Completing part one of the triage form

After creating the file, the first part of the triage form must be completed by the receiving officer as follows:

1. Read through the privacy matter notification.
2. Identify whether the matter is a privacy breach or a privacy complaint.

3. Complete the basic information table based on information received in the privacy matter notification.
4. Complete jurisdictional questions.
5. The receiving officer must note their name, date and signature (can be electronic) on the first line of the approval section at the bottom of the first page.
6. Provide the assessing officer the triage form and access to the folder for further action.

Complexity classifications

The level of complexity is defined in the Classification table on the triage form. It is also outlined in this procedure for additional clarity.

Minor	Assessed as having **negligible risk** or detriment to QCS, stakeholders, and/or affected individuals in relation to non-compliance with the IP Act. **Requires no investigation.**
Standard	Assessed with **minimal risk** or detriment to QCS, stakeholders, and/or affected individuals in relation to non-compliance with the IP Act. **Requires minimal investigation.**
Intermediate	Assessed with **medium level of risk** or detriment to QCS, stakeholders, and/or affected individuals in relation to non-compliance with the IP Act. **Requires detailed investigation.**
Complex	Assessed with **serious or significant level of risk** or detriment to QCS, stakeholders, and/or affected individuals in relation to non-compliance with the IP Act. **Immediate action required. High level investigation required and immediate referral to executive management.**

Further information and examples on the types of issues that would occur under each of these criteria are outlined in the Action and Classification tables on the triage form. Please note, privacy matters may be reclassified at any time throughout the investigation process, for example, based on investigation findings or new information.

Assessing complaint or breach complexity

Once it is confirmed that the matter meets the meaning of a privacy breach or complaint, and a file has been created, the assessing officer must determine the complexity of the matter using the triage form as follows:

1. Read through the information received about the matter.
2. Mark the boxes for the relevant IPPs applying to the matter, based on the information available at the time of assessment.
3. Ensure the information is saved in the relevant file.
4. Use the Classification and comments section to determine the complexity of the alleged privacy breach and select the relevant classification.
5. Use the Classification table to assist in determining the level of the alleged breach. If it is not clear what level classification should be attributed to the alleged breach, err on the side of caution and upgrade the classification to ensure the alleged breach is managed appropriately. Advice can also be obtained from a more senior officer or the Legal Strategy and Services Group. If any information cannot be contained, the classification should automatically be upgraded to Complex due to the associated risks. In relation to an alleged breach where the information was contained, Standard would be selected as below:

Action	Minor	Standard	Intermediate	Complex
Containment	Involves only a use rather than a disclosure of personal information	Limited distribution of information and still under the control of QCS. Information has been contained.	Wider distribution of information and the potential for further disclosure of use.	Information cannot be contained.

6. The RTI and Privacy Group will consult with Professional Standards and Governance Command in instances where it is suspected a QCS officer has acted in a way described in category 3 of the *Conduct and Performance Excellence (CaPE) framework*, or where corrupt conduct has otherwise been identified. The RTI and Privacy Group will be specifically mindful of compromising another investigation.

7. The RTI and Privacy Group will make an initial assessment of the matter to identify any human rights issues by referring to the *Human Rights Act 2019*. If it is identified that the matter has a human rights component, the matter may be actioned by the RTI and Privacy Group, or referred back to the business area responsible for the function responsible for the breach.
8. If at the initial assessment stage it is considered that the matter may be a result of a cyber security incident, notification will occur to the QCS Cyber Security Unit, Digital Services and Information Technology Command (DSITC) and a decision will be made as to whether to enact the cyber security incident response plan and associated playbook.
9. Any matters involving disclosures under the *Public Interest Disclosure Act 2010* will be referred to the Professional Standards and Governance Command and managed in accordance with QCS's *Public Interest Disclosure Policy*.
10. Consideration should be given to briefing senior executives responsible for the relevant business area, particularly is risk mitigation is required to prevent further breaches.
11. The assessing officer must identify the classification type and note their name, date and signature (can be electronic) next to "Assessed by" in the approval section at the bottom of the first page. The assessing officer may also be the receiving officer.
12. The completed triage form must be submitted to the approving officer. The approving officer must be more senior than the assessing officer.

Triage form timeframes

The triage form must be submitted by the assessing officer to the approving officer within two (2) business days from the date the privacy complaint or breach is received by the receiving officer.

The approving officer must approve the triage form within three (3) business days from the day the assessing officer submits the completed triage form to the approving officer.

These timeframes may be adjusted in exceptional circumstances with the agreement of the Manager, RTI and Privacy Group.

Privacy complaint – acknowledgement

A written acknowledgment letter of the receipt of an individual's privacy complaint will be sent to the complainant within five (5) business days of receipt of their complaint by the RTI and Privacy Group.

As mentioned above, complaints about issues other than privacy will be managed and referred to other areas of QCS in accordance with the *Client Complaint Management Policy*, *Individual Grievances People Capability Policy* or the *Public Interest Disclosure Policy as* appropriate, and the complainant informed and provided with contact details for other relevant areas.

The acknowledgement letter must:

- assure the complainant that their feedback/complaint is valued;
- define the scope of the complaint;
- request any further information necessary to action the complaint, including providing the complainant with an opportunity to identify a resolution for the complaint;
- outline how the complaint will be managed, including a timeframe for resolution;
- provide contact details for the QCS officer managing the complaint and;
- advise the complainant about how their personal information will be used and disclosed as part of the investigation.

A response will be provided to the complainant within 45 business days from the date the complaint is received, unless further information is required to properly assess the complaint, in which case a response will be provided within 45 days of the further information being received. The acknowledgement letter will advise the complainant of this.

Investigating the complaint or breach

Each investigation is unique, so the order and extent of an officer's approach to each investigation may vary depending on the specific factors of the complaint or breach.

Privacy complaints will be dealt with fairly and objectively, and in accordance with natural justice principles. Unless the seriousness or complexity of the matter requires otherwise, the investigation process will be undertaken with as little formality as possible and in the spirit of collaboration, business improvement and

complaint resolution.

Identify the scope of the investigation

Examine the information and the triage form to identify the legislative issues enlivened by the complaint or breach. This will enable the investigating officer to gain a clear understanding of what issues fall within the scope of the investigation.

Resolution of a complaint

If the matter is a complaint, identify the complainant's expected outcome, and whether this can be achieved by QCS. If the complainant has not proposed a resolution, provide the complainant with an opportunity to identify a resolution for their complaint. The types of resolutions which may be able to be achieved include:

- providing specific officers or business units with targeted training on the IP Act
- a letter of apology
- a change in business practices.

Investigation planning

Where an investigation is required, the investigating officer must begin planning by identifying information to be sought from officers and business units in order to reach a conclusion on the matter. This does not need to be a formal process. There are a number of questions that the investigating officer may consider in order to gather information to identify whether a privacy breach has occurred.

The following is a non-exhaustive list of matters which the investigating officer may wish to consider when deciding on the types of information they require to reach a view on the matter:

- Which business units are relevant to the alleged privacy breach?
- Is the allegation about the conduct of one or more officers? If so, who are the relevant officers; and who is their line manager?
- If QCS officers have been identified as being able to assist an investigation by providing evidence, how can those officers be best contacted to invite them to an interview?
- Immediate preservation of evidence, for example, any CCTV footage.
- The availability of interviewees.
- Whether relevant supervisors or managers must also be contacted for further information or to attend an interview.
- Any special access requirements that must be addressed, for example, whether access clearance is required for the investigating officer, recording equipment, disability services, or translation services.
- Whether it is a matter which requires consultation with Professional Standards and Governance Command; People Capability Command; and/or QCS Cyber Security Unit, DSITC.
- Whether it is likely that the investigation process will exceed 45 business days. If so what contingency plans are in place and who needs to be notified of this?
- What evidence already exists and in which form, for example CCTV footage, photographs, documents, soft copy files, emails? How can that evidence be obtained?
- Whether external evidence is required, for instance, from another government department, a private individual, or an external supplier.
- Whether technical expertise or other expert assistance is required.
- What, if any, contingency plan can be put in place if an officer or other individual who can assist the investigation refuses or otherwise is unable to take part in an interview.
- Whether evidence can be obtained by some other method, for example, by way of a written and signed statement.

Requesting information from relevant parties

The investigating officer may contact individuals relevant to the matter (including QCS officers) and invite them to attend an interview about the alleged breach. If the individual is subject to any disciplinary investigations or proceedings in relation to the matter, or the individual refuses to be interviewed, legal advice should be obtained.

A record of any interview conducted must be made. These records can be in an audio electronic form or written as contemporaneous file notes during the interview. For more serious matters, interviews should be electronically recorded.

Documenting information

When information about the privacy breach or complaint is received from relevant parties, ensure that CMS is updated accordingly with the information and time spent on the matter.

Evaluation of the evidence

Once the evidence has been received from the relevant parties, determine the weight to be applied to it. The standard of proof used is the civil standard of proof – the balance of probabilities.

That is, that the complaint is made out or confirmed to have more likely than not occurred.

Privacy complaint – outcome

Where a privacy complaint is substantiated, the investigating officer must have regard to the complainant's suggestion for resolution (if any).

Remedies which may be available to the complainant include:

- a written or verbal apology
- an explanation as to how or why the breach occurred
- organisational change such as changes to policies, procedures or operational practices
- privacy training for the relevant officers and business unit.

A report will be prepared outlining the complaint, its assessment and investigation and its recommended resolution. The report will be submitted to the approving offer and include all relevant dates to demonstrate the requisite timeframes have been met.

Privacy complaint – response

The approving officer will consider the privacy complaint and decide on the most appropriate remedy, having regard to the relevant and reliable evidence and affected person/s submissions. Any response to the complainant must include:

- the outcome of the investigation
- the decision of the relevant officer, including whether the complaint was substantiated or not
- a clear explanation of how the decision was made and the information relied upon to make that decision
- information about any changes implemented as a result of the complaint
- where the matter relates to a serious data breach, provide guidance in consultation with the QCS Cyber Security Unit to the complainant on the steps they may take to limit the harm arising out of the breach
- any resolution to the complaint if substantiated, as outlined in the section above
- information about the complainant's right under Sections 165(1) and 163 (3) of the IP Act to make a complaint to the OIC if they consider QCS's response to their complaint not to be an adequate response.

Finishing the file

Before finalising the file, ensure that all information has been accurately and correctly documented both in CMS and the folder file, and any evidence stored or returned.

Consider any systemic issues identified

There may be circumstances where an investigation into a privacy matter indicates that the breach occurred because a procedure, policy or business practice was insufficient to protect and manage personal information in line with the IPPs; insufficient secure storage of personal information; lack of information security, cyber security, and privacy training to staff; or a cyber security breach.

Where an investigation indicates that a privacy breach has occurred, the investigating officer may recommend that the business unit review and update its business practices and include any of the following:

- privacy training to the relevant individual and/or work unit

- amendment of policies, forms and/or collection notices to ensure clear guidance and compliance with the IPPs
- providing additional accessible information to ensure privacy concepts are understood
- improve security and storage measures in accordance with IPP 4
- steps to improve data accuracy in accordance with IPP 4 and the Queensland Government Enterprise Architecture IS18 Information Security Policy (IS18:2018).

Definitions

Term	Definition/explanation
Approval table	Contains information about the receipt, assessment and approval of a triage assessment undertaken in relation to a privacy complaint or privacy breach.
Classification table	A table containing information about the different types of privacy breaches and issues raised in privacy complaints, and the risks/harm to QCS, stakeholders, complainants, and other individuals as a result of these issues. The table identifies the level of investigation required.
Serious data breach	A data breach that is likely to result in serious harm to an individual from the perspective of a reasonable person in QCS's position. Serious harm includes serious physical, psychological, emotional, financial or reputational harm (refer to Office of the Australian Information Commissioner website).

Document information and review

Security classification:	Official	Review frequency:	Three (3) years*

*An administrative review of this document should be conducted every three years, or at times of critical content changes. In light of amendments made by the *Information Privacy and Other Legislation Amendment Act 2023*, this document will also be reviewed prior to 1 July 2025.

Current version:	Effective date:	Notes:	Next review due:
1	1 March 2021	Removed content not relevant to QCS (i.e. DJAG). Rebadged to align with current QCS corporate identity guidelines.	2024
2	7 March 2024	Changing to wording (clarifying breaches and complaints), storage (e.g. hard folders no longer required), formatting.	2025
3	4 July 2024	Changes resulting from internal consultation.	2025