# Data Breach Policy

| | | |
|---|---|---|
| **Owner:** | **Legal** | **CS/LEG/0008** |
| **Last reviewed:** | **06/08/2025** | **Version: 1.00** |

## 1 Purpose

This policy sets out how the Queensland Academy of Sport (QAS) will respond to data breaches, including 'suspected eligible data breaches' under the Mandatory Notification of Data Breach (MNDB) scheme under the *Information Privacy Act 2009* (IP Act).

While not all data breaches will be 'eligible data breaches', QAS takes all data breaches seriously and will assess each data breach in accordance with this policy.

This policy is supported by the following documents:

- Data Breach Response Report
- Data Breach Register
- Information Privacy Policy.

## 2 Statement

### 2.1 Data breach classifications

#### 2.1.1 Data breach

A data breach is defined in the IP Act to mean the unauthorised access or disclosure of information held by an agency or the loss of personal or non-personal information held by an agency where unauthorised access or disclosure is likely to occur.

A data breach may occur as the result of a malicious action, systems failure or human error. A data breach may occur also because of misconception as to whether a particular act or practice is permitted under the IP Act.

#### 2.1.2 Eligible data breach

An **eligible data breach**, according to section 47(1) of the IP Act, is a data breach which has satisfied the following two tests under the MNDB Scheme:

- *always* involves personal information, and
- involves an actual or potential loss of, unauthorised access to, or unauthorised disclosure of personal information, which is "likely to result in serious harm" to one person or more.

| Examples of eligible data breaches include: | Examples of less serious data breaches include |
|---|---|
| • A worker accidentally losing or misplacing documents containing sensitive or personal information<br>• A contractor disclosing sensitive personal information to external partners<br>• An online internal database or portal is accidentally made publicly available<br>• Inappropriate access by a staff member or individual to a restricted internal file containing sensitive personal information<br>• A cyberattack, phishing, malware or hacking incident into an agencies database allowing access by external parties | • Sending a generic email to the wrong recipient (only a few unintended recipients)<br>• Accidentally accessing a secure database<br>• Disclosing agency information to third parties on an unauthorised basis<br>• Leaving an encrypted USB or computer containing contact details such as emails addresses of staff on a train |

### 2.1.3 Suspected eligible data breach

A **suspected eligible data breach** occurs when an agency has reasonable grounds to suspect that a data breach may have happened but has not yet confirmed that it meets the criteria for an eligible data breach.

## 2.2 Potential impacts of a data breach

The impact of a data breach depends on the nature and extent of the breach and the type of information that has been compromised.

Serious impacts of a breach could include:

- Risks to individuals' safety
- Financial loss to an individual or organisation
- Damage to personal reputation or position
- Loss of public trust in QAS
- Commercial risk through disclosure of commercially sensitive information to third parties
- Threat to QAS systems, leading to disruption of activities
- Impact on QAS reputation, finances, interests or operation.

It is important to note that breaches of personal data can result in significant harm, including people having their identity stolen or the private home addresses of vulnerable people being disclosed. As such, even a breach affecting an individual or a small number of people may have a large impact.

## 2.3 What is the Mandatory Notification of Data Breach (MNDB) scheme?

The MNDB scheme requires agencies to take the following prescribed actions in responding to data breach, including an 'Eligible Data Breach':

- immediately take all reasonable steps to contain and mitigate the data breach;

- if the agency does not know if the data breach is an ‘Eligible Data Breach’, it must assess, within 30 days, whether there are reasonable grounds to believe that the data breach is an ‘Eligible Data Breach’;
- notify other affected agencies; and
- if the agency knows or assesses the data breach as an ‘Eligible Data Breach’, notify the Office of the Information Commissioner (OIC) and any individuals whose personal information is the subject of the data breach, unless an exemption to notification applies.

## 2.4 Preparing for a potential data breach

Preparation is critical to ensuring QAS is ready to respond effectively to data breaches.

The following documents outline QAS’s key controls, systems and processes for responding to a data breach:

- Data Breach Response Plan and Report
- QAS Critical Incident Management Plan (CIMP)
- QAS Business Continuity Plan (BCP)
- Information Technology Partners (ITP) Cyber Incident Response Plan
- ITP Disaster Management Plan
- ITP Incident Response Procedure.

The Senior Leadership Team are responsible for ensuring that staff complete relevant training on code of conduct, privacy, data, information and cyber security and are aware of the obligations and requirements under this policy.

## 2.5 Responding to a data breach

While every data breach incident is different and will require a different response, QAS is committed to a structured and effective response using the following six stage approach to minimise harm, comply with legal obligations, and improve future data protection practices.


### 2.5.1 Stage 1: Alert and contain

Where a data breach is known to have occurred (or is suspected) any QAS worker who becomes aware of the breach must immediately alert (by phone or in person) the Privacy Officer and their line manager.

Where possible, the worker who discovered the breach should try and provide the following information:

- Contact name and number of persons reporting the incident
- The type of data or information involved
- Whether the loss of the data puts any person or other data at risk
- Location of the incident

- Date and time the breach occurred
- Location of data or equipment affected
- Type and circumstances of the incident.

It is important to note that the worker who discovered the breach should raise the alert immediately and not wait until all the key details on the breach have been established.

If the worker who discovers the breach is authorised to take action to contain the breach, they must act as soon as possible to contain the breach and minimise the damage.

What is reasonable will depend on the circumstances of the data breach and QAS will consider containment methods proportionate to the size and scale of QAS and the type of information it collects.

Some steps include:

- Immediately take whatever steps possible to contain the breach and minimise any resulting damage. For example, recover the information, including any copies, shut down the system that has been breached, suspend the activity that led to the data breach, revoke or change access codes or passwords.
- If a third party is in possession of the personal information and declines to return it, it may be necessary to seek immediate legal advice on what action can be taken to recover the information. When recovering information, ensure copies have not been made or that all copies are recovered.
- Take the following steps to contain an email that has been sent or copied to the wrong recipient:
    1. find out whether the recipient has read, printed or forwarded the email
    2. confirm that the email has been deleted by the recipient
    3. liaise with the recipient's IT department to confirm the email and any backups have been deleted from the system
    4. notify the Privacy Officer as soon as possible.
- Be careful when containing the breach not to destroy information that may be needed to investigate the cause of the breach.

Please note that not all workers will be authorised to take these actions, and containment should only be enacted by authorised workers.

### 2.5.2 Stage 2: Verify

Once notified of any data breach, the Privacy Officer will quickly establish the key details of the breach, including when it occurred or was identified, how it occurred, what data was affected and the extent of the breach. The Privacy Officer will also consider whether the data breach involves personal or health information and provide findings to the Executive Director Corporate Services. For all data breaches that occur via electronic means, the Privacy Officer will also notify the Digital Services Manager who can begin activities to support containment in line with relevant policies.

The Executive Director Corporate Services may stand up a Data Breach Response (DBR) Team where necessary. Depending on the nature of the breach, membership may include the Privacy Officer, the Digital Services Manager, Communications and Media, Human Resources, Legal Counsel and senior staff from the relevant business area. The DBR Team will task key personnel with roles for assessment and notification of decision, overseeing reporting obligations and post-breach review.

Where the incident triggers two or more policies, such as the data breach policy and BCP, the Executive Director Corporate Services will assess upon advice from relevant areas and make directions on response strategy to ensure efficiency in response and avoid duplication. Any decisions in respect of this will need to ensure that all relevant policies and legislative requirements have been complied with.

### 2.5.3 Stage 3: Rectify

The DBR Team must take steps to eliminate the circumstances enabling the breach. This could include actions such as initiating take down orders on external websites or putting processes in place to assist individuals who have been affected by the breach. The steps of the rectification process must be recorded in the Data Breach Response Report.

### 2.5.4 Stage 4: Assess

QAS will comprehensively assess the risks associated with the breach, including an assessment as to whether the data breach is an Eligible Data Breach for the purposes of the IP Act and the MNDB scheme.

The OIC's MNDB assessment tool can assist in assessing the risk of harm to individuals as a result of the data breach. The risk assessment is recorded in the Data Breach Response Report and escalated to managers, the Privacy Officer and the Digital Services Manager where appropriate so that relevant business continuity responses and measures can be enacted.

The assessment stage focuses on an assessment being conducted, within 30 days of forming a reasonable suspicion of a data breach, under section 48(2)(b) of the IP Act. Section 48(2)(b) of the IP Act also deals with the prospect that when a data breach is first identified, agencies may not have sufficient information to reach a level of certainty that the data breach is an Eligible Data Breach. Where this occurs and QAS only has a reasonable suspicion of an Eligible Data Breach, there is a requirement to rapidly assess whether there are reasonable grounds to believe the data breach is an Eligible Data Breach.

However, if QAS is satisfied that it will be unable to complete the assessment in 30 days, it can extend that time under section 49 of the IP Act.

### 2.5.5 Stage 5: Notify

There are requirements under sections 51 to 54 of the IP Act to include a clear notification strategy which enables quick and effective communication with the Information Commissioner, affected individuals and other external parties as required. QAS will collect sufficient information about the breach before issuing notifications. Premature notifications are not recommended and may cause unnecessary harm, panic and concern.

#### 2.5.5.1 Notifying the Information Commissioner

| | |
|---|---|
| When | Unless an exemption applies, the Information Commissioner must be notified as soon as practicable after forming the belief that a data breach is an Eligible Data Breach. |
| How | Notification of an Eligible Data Breach must be made in writing. |
| What | Refer to section 51 of the IP Act. |

### 2.5.5.2 Notifying affected individuals

| | |
|---|---|
| When | Unless an exemption applies, QAS will take the steps set out in section 53 of the IP Act to notify particular individuals as soon as practicable after forming a reasonable belief that a data breach is an Eligible Data Breach. |
| How | How affected individuals/organisations affected by the 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.<br><br><u>Option 1: Notify each individual</u><br><br>If it is reasonably practicable to notify each individual whose personal information was accessed, disclosed or lost, QAS will take reasonable steps to notify each individual of the required information directly. This may include by telephone, letter, email or in person.<br><br><u>Option 2: Notify each affected individual</u><br><br>If Option 1 does not apply, QAS will take reasonable steps to notify each affected individual of the required information for the data breach, if doing so is reasonably practicable.<br><br>Under sections 47(1)(a)(ii) and (b)(ii) of the IP Act, an 'affected individual' is someone to whom the personal information relates, and who is likely to suffer serious harm as a result of the data breach.<br><br><u>Option 3: Publish Information</u><br><br>If QAS cannot directly notify each individual (Option 1) or each affected individual (Option 2), it will publish the required information on the QAS website for a period of at least 12 months, in accordance with section 53(1)(c) of the IP Act. QAS is not required to include information in its notice if it would prejudice its functions. QAS will advise the Information Commissioner how to access the notice and the Commissioner is required to publish the notice on the Commissioner's website for at least 12 months. |
| What | Refer to section 53(2) of the IP Act. |

### 2.5.5.3 Notifying other entities

While not required by the IP Act, in some circumstances it may be appropriate to notify other entities of a data breach, for example:

- if the breach involves 'corrupt conduct' within the meaning of the *Crime and Corruption Act 2001*, the Crime and Corruption Commission Queensland must be notified;
- requirements to report cyber and information security incidents to Queensland Government Information Security Virtual Response Team according to the Business Impact Level;
- if the breach appears to involve theft or other criminal activity, the Queensland Police Service (QPS) should be notified as a matter of course. The QPS website has links and assistance to report cybercrime and other offences;
- entities with obligations under the *Privacy Act 1988* (Cth) National Data Breach (NDB) Scheme (e.g. Tax File Number recipients) may be obliged under the NDB scheme to report the breach to the Office of the Australian Information Commissioner.

Depending on the circumstances of the data breach and the information involved, other notification may be appropriate. For example, QAS's portfolio Minister, financial institutions or credit card companies, or professional or other regulatory bodies.

It should be noted that the above reporting obligations and considerations may apply to *any* breach or compromise of *any* type of information, and not only to those assessed as eligible data breaches under the MNDB scheme.

#### 2.5.5.4 Who should notify?

The CEO will make notifications relating to data breaches by QAS. This will ensure that the notification is made in accordance with QAS's media provisions and the feedback from affected individuals or organisations can be received directly. The Minister's office may also need to be consulted. If required, the Communications and Media team will assist in developing a communications plan as outlined in the CIMP.

#### 2.5.5.5 Exemptions from notification obligations

Chapter 3A, Part 3, Division 3 of the IP Act sets out the circumstances in which an agency is not required to comply with the notification obligations, including where:

- complying with the obligation would be likely to prejudice an investigation that could lead to the prosecution of an offence or proceeding before a court or tribunal;
- the eligible data breach involves more than one agency, and another agency is undertaking the notification obligations;
- the agency has taken specified remedial action under section 57;
- compliance would be inconsistent with a provision of an Act of the Commonwealth or a State that prohibits or regulates the use or disclosure of the information;
- compliance would create a serious risk of harm to an individual's health and safety; and
- compliance is likely to compromise or worsen the agency's cybersecurity or lead to further data breaches of the agency.

### 2.5.6 Stage 6: Review

After a data breach has been dealt with, a post-incident review and remediation process will be undertaken by the DBR Team to ensure key learnings are identified, and (where possible) improvements and other remediation activities are implemented.

Where the data breach has occurred via electronic means, the review will incorporate consultation with the Digital Services Manager and ITP to ensure a broadened view of cause and response.

The review may include:

- Incident Review: Analysing the root cause of the breach and evaluating the effectiveness of the response.
- Policy and Process Updates: Updating policies, procedures, or systems to address vulnerabilities and prevent future breaches.
- Staff Training: Providing additional training to staff to reinforce data protection practices and breach response protocols.
- Monitoring and Reporting: Monitoring for any ongoing risks or issues and reporting outcomes to Senior Leadership Team.

The completed Data Breach Response Report will be submitted to the CEO and Board by the Privacy Officer for noting.

## 2.6 Register of Eligible Data Breaches

QAS maintains an internal Register of Eligible Data Breaches in accordance with section 72 of the IP Act. This register serves as a formal record of all eligible data breaches, ensuring compliance with legislative requirements and supporting QAS's commitment to transparency, accountability, and continuous improvement in data protection practices.

The Privacy Officer is responsible for maintaining the Register and may seek required information from relevant areas.

# 3 Authority

*Information Privacy Act 2009*

Information Privacy Act 2009 - QPP 1

Information Privacy Regulation 2009

*Right to Information Act 2009*

*Public Sector Act 2022*

*Public Sector Ethics Act 1994*

*Human Rights Act 2019*

Queensland Public Service Code of Conduct

# 4 Scope

This policy applies to all persons who perform work for QAS including:

- Employees
  - permanent, fixed-term and temporary
  - secondees from other agencies (including staffing approved under interchange or mobility arrangements)
    - work placement staff (such as trainees, work experience students, cadets)
    - PhD students (engaged via a university contract)
    - non-executive employees engaged via a fixed term contract
  - senior officers and senior executives including those engaged via a section 155 contract remunerated at SES level or above.
- Contractors
  - sub-contractors
  - consultants
  - their employees (including labour hire staff) who are engaged via contract or agreement.
- QAS Board

*Note: For application of this policy and supporting documents, the term 'worker' is used collectively to describe persons who perform work for QAS.*

# 5 Delegations

Delegations in relation to this document are to be exercised in accordance with the QAS Human Resource Delegation Instrument and Financial and Contractual Delegation Instrument.

*Note: Delegation Instruments are reviewed on a regular basis to ensure they remain current and relevant to operational needs. It is recommended that delegate authority levels are confirmed prior to exercising any powers.*

# 6 Responsibilities

**Chief Executive Officer:**

- Is the 'principal officer' in relation to the operation of the IP Act.
- With support of the Executive Director Corporate Services, ensure the QAS Data Breach Policy is relevant and complies with the IP Act and MNDB Scheme.
- Make notifications in relation to data breaches and eligible data breaches with support from the Privacy Officer.

**Executive Director Corporate Services:**

- Promotes compliance with the MNDB Scheme.
- Stand up a Data Breach Response Team where required.
- Where two or more policies apply, make decisions on a response strategy which ensures efficiency and avoids duplication.

**Data Breach Response Team:**

- Members are nominated by the Executive Director Corporate Services.
- Manage a data breach that is considered likely to cause serious harm to any impacted individual or the agency's systems.
- Undertake post-incident review.

**Privacy Officer:**

- Assess the severity of a data breach involving personal information and the likelihood that a breach will result in serious harm to an individual to whom the information involved relates.
- Immediately report a data breach that is also a cyber security incident to the ITP Chief Information Officer, and Chief Information Security Officer via the Digital Services Manager, if not already reported.
- Escalate serious data breaches to relevant senior officer or executive.
- Assist the Executive Director Corporate Services in coordinating the QAS response including standing up and supporting a Data Breach Response Team.
- Arrange for the Chief Executive Officer to notify the Information Commissioner, affected persons and others where required. This includes publishing, monitoring and reviewing the currency of public notifications of a data breach published to the QAS website under section 53(1)(c). The Communications and Media team and the Minister's office may need to be consulted.
- Maintain the Register of Eligible Data Breaches.

**Digital Services Manager:**

- Immediately report a cyber security incident that is also a data breach to the Privacy Officer and Executive Director Corporate Services, if not already reported.

- Notify and report to the ITP Chief Information Officer and Chief Information Security Officer who will assist in coordination and reporting requirements with the Queensland Government Cyber Security Unit.
- Implement the ITP Cyber Incident Response Plan and related cyber security management procedures if the data breach is also cyber security incident.

**Senior Leadership Team**

- Ensure that staff complete relevant training on code of conduct, privacy, data, information and cyber security and are aware of the obligations and requirements under the data breach policy.

**Manager**

- Identify and escalate concerns within area of responsibility which may enliven the requirements of this Data Breach Policy.
- Immediately report a data breach to the Privacy Officer, if not already reported.

**All employees:**

- Any QAS worker who becomes aware that a data breach has occurred (or is suspected) must immediately alert (by phone or in person) the Privacy Officer and their line manager.
- Read the Data Breach Policy and understand what is expected of them.
- Complete all relevant training.
- Comply with the IP Act, including protecting personal information held by QAS from unauthorised access, disclosure or loss.
- Respond to requests for information from and cooperate with the Privacy Officer and/or the Data Breach Response Team.
- Comply with record keeping obligations.

# 7 Reporting requirements

- Serious data breaches and remedies applied are reported yearly in the QAS annual report, in accordance with the *Public Records Act 2023*.

Per section 63 of the *Financial Accountability Act 2009* and section 21.4 of the Annual report requirements for Queensland Government agencies, Ministers are required to table annual reports for their portfolio agencies and statutory bodies in the Queensland Legislative Assembly by 30 September each year.

# 8 Storage of information

All information will be managed in accordance with the:

- *Public Records Act 2023*
- *Queensland Government Recordkeeping and Information Management Framework*
- *Queensland Government Records Governance Policy*

In addition, personal information will be managed in accordance with the *Information Privacy Act 2009*, in particular the Queensland Privacy Principles (QPPs) in that Act.

# 9 Complaints management

A person who is dissatisfied with, and is directly affected by, a service, action or decision made by QAS, its staff or persons it has engaged to provide services may lodge a complaint in accordance with the *Public Sector Act 2022* and relevant QAS policies and procedures.

If a complainant is dissatisfied with any action taken by QAS in relation to a complaint, and after they have exhausted all available avenues of review within QAS as outlined in the Complaint Management Policy, they can request for QAS's decision to be reviewed by the Queensland Ombudsman.

# 10 Employee grievances and appeals

An employee who is the subject of an administrative decision or action is entitled to lodge a complaint in accordance with the Managing Employee Grievances Policy should they feel the administrative decision is unfair or biased.

Employees who are unsatisfied with the outcome of their employee complaint may be entitled to lodge an appeal in accordance with PSC Appeals Directive 04/23.

An appeal may be started by giving the Industrial Registrar an appeal notice. Further information on starting an appeal and appeal rights is available from the Queensland Industrial Relations Commission website.

# 11 Human rights considerations

This document is compatible with human rights under the *Human Rights Act 2019* because it limits a human right only to the extent that is reasonable and demonstrably justifiable in accordance with section 13 of that Act.

This document was last reviewed in 06/08/2025 to ensure actions and decisions under the policy are made in a manner compatible with human rights. Please note, when implementing this policy, workers must still consider if any human rights are relevant to and likely to be impacted by a particular decision, and whether any limitation of human rights are reasonable and justified.

# 12 Definitions

| Word/Term/Acronym | Meaning |
|---|---|
| Affected individual | An "affected individual" under section 47(1)(ii) of the IP Act. |
| Data Breach | The unauthorised access to, or unauthorised disclosure of information or the loss of information in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur in accordance with schedule 5 of the IP Act. |
| Eligible Data Breach | An "Eligible Data Breach" will have occurred under section 47 of the IP Act where:<br>a) there has been unauthorised access to, or unauthorised disclosure of **personal information** held by an agency, **and**<br>the access or disclosure is likely to result in **serious harm** to any of the **individuals** to whom the information relates; **or**<br>b) there has been loss of **personal information** held by an agency that is likely to result in unauthorised access to, or unauthorised disclosure of the personal information, **and** |

| Word/Term/Acronym | Meaning |
|---|---|
| | the loss is likely to result in **serious harm** to any of the **individuals** to whom the information relates. |
| Information Commissioner | Depending on the nature of the data breach:<br>• The Queensland Information Commissioner, and/or<br>• The Australia Information Commissioner |
| Personal information | According to section 12 of the IP Act, personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion—<br>(a) whether the information or opinion is true or not; and<br>(b) whether the information or opinion is recorded in a material form or not.<br>Personal information does not include:<br>• information about a person whose identity is not known or who cannot be readily identified (deidentified information)<br>• information about a deceased person - whilst private in nature, it is not considered personal information for the purpose of the IP Act<br>• information about a company (however, it does apply to personal information about an employee of that company)<br>routine personal work information for public sector employees. |
| Privacy Officer | Legal Counsel has been designated as the Privacy Officer. |
| Sensitive information | According to schedule 5 (Dictionary) of the IP Act, sensitive information for an individual, means the following:<br>a) information or an opinion, that is also personal information, about the individual's—<br>i) racial or ethnic origin<br>ii) political opinions<br>iii) membership of a political association<br>iv) religious beliefs or affiliations<br>v) philosophical beliefs<br>vi) membership of a professional or trade association<br>vii) membership of a trade union<br>viii)sexual orientation or practices<br>ix) criminal record<br>b) health information about the individual;<br>c) genetic information about the individual that is not otherwise health information;<br>d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or<br>e) biometric templates. |
| Serious harm | To an individual in relation to the unauthorised access or unauthorised disclosure of the individual's personal information, includes, for example: |

| Word/Term/Acronym | Meaning |
|---|---|
| | a) serious physical, psychological, emotional or financial harm to the individual because of the access or disclosure, or<br>b) serious harm to the individual's reputation because of the access or disclosure.<br>Section 47(2) of the IP Act prescribes factors to consider when assessing whether the likely harm is 'serious harm'. These factors include the kind of personal information disclosed, sensitivity of the personal information involved and the persons who have or may have obtained the personal information subject to the breach. |

# 13 Date of effect and review

This policy and its supporting documents:

- come into effect from the date of delegate approval
- will be reviewed within two years of the approval date unless otherwise:
  - stipulated in statutory obligations
  - triggered by circumstances determined appropriate by QAS.

# 14 Delegate approval

| |
|---|
| DAVID LYONS<br>**Chairperson**<br>Queensland Academy of Sport Board |
| Date: 06 August 2025 |

# 15 Version history

| Version | Date | Author | Amendment description | Action |
|---|---|---|---|---|
| 1.00 | 6/08/2025 | Corporate Services | New document | Approved by the Board |