Data Breach Plan

1. Purpose

The purpose of this Data Breach Plan is to set out how TAFE Queensland will respond to data breaches in accordance with the Mandatory Notification of Data Breach Scheme under the *Information Privacy Act 2009 (Qld)*.

2. Overview

TAFE Queensland is committed to protecting personal information including sensitive information and ensuring timely and effective management of data breaches in accordance with the *Information Privacy Act 2009 (Qld)* and other applicable legislation.

Plan Principles:
Principle 1: TAFE Queensland will promptly identify and assess suspected data breaches.

Principle 2: TAFE Queensland will take appropriate steps to contain, investigate, and remediate data breaches.

Principle 3: TAFE Queensland will notify affected individuals and relevant authorities where required.

Principle 4: TAFE Queensland will maintain a register of eligible data breaches and continuously improve its data protection practices.

Principle 5: TAFE Queensland will uphold human rights in its response to data breaches, including the right to privacy and protection of vulnerable individuals.

Accountability:
The Chief Information Officer is accountable for ensuring the management and maintenance of this plan, including ensuring its continued appropriateness to the business, compliance with legislation and external requirements, and periodic review.

TAFE Queensland Executives are responsible for managing data breach incidents under the terms of this policy.

3. Audience

3.1 This plan applies to TAFE Queensland's:

	☒ TAFE Queensland Core Staff

4. Plan

Application:

4.1 This plan applies to:

- **(a)** all actual and suspected data breaches involving personal information, whether accidental or deliberate that occur within TAFE Queensland information assets, physical records or third-party services; and
- **(b)** All staff and contractors who handle TAFE Queensland personal information.

Human Rights Considerations:

4.2 Several human rights protected under the *Human Rights Act 2019 (Qld)* are directly relevant to data breaches and the handling of personal information:

- **(a)** Privacy and Reputation (Section 25): Every individual has the right not to have their privacy, family, home, or correspondence unlawfully or arbitrarily interfered with;

(b) Protection of Families and Children (Section 26): If a data breach involves sensitive information about children or families, additional care must be taken to protect their rights;
(c) Right to Life (Section 16): In extreme cases, a data breach could endanger someone's life (e.g., if sensitive information about a person in a protected witness program is disclosed); and
(d) Equality Before the Law (Section 15): TAFE Queensland must ensure that its response to data breaches does not unfairly disadvantage vulnerable groups.

Reporting a Data Breach:

4.3 Staff must report all suspected data breaches immediately via TAFE Queensland's IT Service Management (ITSM) tool and to their manager.

4.4 Members of the public can report a suspected data breach by using the TAFE Queensland Privacy Feedback Form or contacting TAFE Queensland through its website or by phone.

Responding to a Data Breach:

4.5 TAFE Queensland will follow a six-stage process to respond to data breaches.

Stage 1 - Data Breach Preparations:

4.6 TAFE Queensland has prepared for a data breach by:
(a) Maintaining an up-to-date *Cyber Security Incident Response Plan* and *Privacy Data Breach Procedure*;
(b) Annual testing of the *Cyber Security Incident Response Plan*;
(c) Conducting regular training for staff on information privacy and cyber security; and
(d) Ensuring robust security measures are in place, including encryption, access controls, and regular audits.

Stage 2 – Identification:

4.7 TAFE Queensland will:
(a) Identify and report suspected data breaches immediately to TAFE Queensland's Cyber Security Team via the ITSM tool;
(b) Conduct an initial assessment to determine whether a data breach has occurred; and
(c) Document the details of the incident, including the date, time, and nature of the breach.

Stage 3 - Containment and Mitigation:

4.8 TAFE Queensland will take immediate steps to:
(a) Contain the breach and prevent further unauthorised access or disclosure; and
(b) Implement measures to mitigate harm.

Stage 4 – Assessment:

4.9 TAFE Queensland will assess the scope and impact of the breach, including:
(a) The type of personal information involved;
(b) The number of individuals affected; and
(c) The potential for serious harm.

4.10 Determine whether the breach meets the criteria for an eligible data breach under the *Information Privacy Act 2009 (Qld)* and the Mandatory Notification of Data Breach Scheme.

Stage 5 – Notification:

4.11 If the breach is deemed eligible, TAFE Queensland will notify affected individuals and the Office of the Information Commissioner Queensland (OIC) as soon as practicable.

4.12 Notifications will include:
(a) A description of the breach;
(b) The type of information involved;
(c) Steps individuals can take to protect themselves; and
(d) Contact details for further information.

4.13 If notification is not required, TAFE Queensland will document the reason for this decision.

Stage 6 - Post Data Breach Review and Remediation:

4.14 Depending on the severity of the data breach, TAFE Queensland may conduct a post-incident review to identify the root cause of the breach and evaluate the effectiveness of the response.

4.15 As necessary, TAFE Queensland will implement corrective actions to prevent future breaches, such as updating policies, improving security measures, or providing additional training.

Register of Eligible Data Breaches:

4.16 TAFE Queensland will maintain a *Register of Eligible Data Breaches*, which will include:

- **(a)** Details of the breach (e.g., date, nature, and scope);
- **(b)** Actions taken to contain and mitigate the breach;
- **(c)** Assessment outcomes and notification decisions; and
- **(d)** Post-incident review findings and remediation actions.

Record Keeping:

4.17 All data breach incidents, whether eligible or not, will be documented and retained in accordance with the *Public Records Act 2023 (Qld)*.

5. Responsibilities

All Staff:

5.1 Report actual or suspected data breaches promptly via the *Report an Information Security Incident Form* in TAFE Queensland's ITSM tool and to their manager.

5.2 Respond to requests for information from, and cooperate with, the Principal Privacy Officer and/or the Breach Response Team.

5.3 Comply with the *Information Privacy Act 2009 (Qld)*, including protecting personal information held by TAFE Queensland from authorised assess, disclosure or loss.

5.4 Comply with record keeping obligations.

Contractors:

5.5 Comply with contractual obligations regarding data protection and breach notification.

Breach Response Team:

5.6 Assemble promptly in response to breaches and will contain, manage and report on data breaches.

5.7 The composition of the Breach Response Team will change depending on the type and severity of the data breach.

Cyber Security Team:

5.8 Assess all data breaches.

5.9 Participate as members or leaders of the Breach Response Team.

5.10 Maintain the *Eligible Data Breach Register*.

Chief Information Officer:

5.11 Ensure TAFE Queensland has planned and is appropriately prepared to manage possible data breaches.

6. Definitions

Affected Individual:
A living individual whose personal information is subject to an eligible data breach.

Data Breach:
An incident where information held by TAFE Queensland is accessed, disclosed, lost, or destroyed without authorisation, potentially causing harm.

Examples of data breaches include:

(a) Malicious or criminal attack:
- i. Cyber incidents such as ransomware, malware, hacking, phishing or access attempts resulting in access to, leakage or theft of personal information;
- ii. Social engineering or impersonation leading into inappropriate disclosure of personal information;
- iii. Insider threats from employees using their valid credentials to access or disclose personal information outside the scope of their duties or permissions; and
- iv. Theft of a physical asset such as a paper record, laptop, removable storage device or mobile phone containing personal information.

(b) System fault:
- i. Where a software bug allows access to a system without authentication, or results in automatically generated notices including the wrong personal information or being sent to incorrect recipients

(c) Human error:
- i. When a letter or email is sent to the wrong recipient;
- ii. When system access is incorrectly granted to someone without appropriate authorisation; and
- iii. When employees fail to implement appropriate password security, for example not reviewing access permissions, securing passwords, or sharing password and log in information.

Eligible Data Breach:
An "Eligible Data Breach" will have occurred under section 47 of the *Information Privacy Act 2009 (Qld)* where:

(a) There has been unauthorised access to, or unauthorised disclosure of personal information held by TAFE Queensland, and the access or disclosure is likely to result in serious harm to any of the individuals to whom the information relates; or

(b) There has been loss of personal information held by TAFE Queensland that is likely to result in unauthorised access to, or unauthorised disclosure of the personal information, and the loss is likely to result in serious harm to any of the individuals to whom the information relates.

Held or Hold (in relation to personal information):
Personal information is held by TAFE Queensland, or TAFE Queensland holds personal information, if the personal information is contained in a document in the possession, or under the control, of the TAFE Queensland.

Mandatory Notification of Data Breach Scheme:
A scheme established under the *Information Privacy Act 2009 (Qld)* which requires management and notification of eligible data breaches.

Personal Information:
Information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion:

(a) Whether the information or opinion is true or not, and

(b) Whether the information or opinion is recorded in a material form or not.

Sensitive Information:
Includes personal information about an individual's racial or ethnic origin, political opinions, religious beliefs, sexual orientation, health information, or criminal record.

Serious Harm:
To an individual in relation to the unauthorised access or unauthorised disclosure of the individual's personal information, includes, for example:

(a) Serious physical, psychological, emotional or financial harm to the individual because of the access or disclosure; or
(b) Serious harm to the individual's reputation because of the access or disclosure.

Unauthorised Access:
Access to data by an individual or entity without permission. Examples include:

(a) An employee browsing records without a legitimate purpose; and
(b) A cyberattack compromising TAFE Queensland systems.

Unauthorised Disclosure:
Disclosure of data to an unauthorised party. Examples include:

(a) Sending personal information to the wrong recipient; and
(b) Publishing sensitive information online without consent.

6. Legislative and Policy Basis

Authority:
Information Privacy Act 2009 (Qld)
Human Rights Act 2019 (Qld)
Privacy Act 1988 (Cth)

Related Policies/Procedures and Other Documents:
Privacy Policy