

Data Breach Policy

Approved by: Managing Director

Approval date: 28 September 2026

Effective date: 29 September 2026

Next review due date: 28 September 2029

Acknowledgement of Country

In the spirit of reconciliation, TAFE NSW acknowledges Aboriginal and Torres Strait Islander peoples as the Traditional Custodians of Country throughout Australia and their connections to land, sea, and community. We pay our respect to Elders past and present and extend that respect to all Aboriginal and Torres Strait Islander peoples today.

Table of contents

Section 1. Purpose.....	2
Section 2. Scope	2
Section 3. Policy statements	2
Data breach prevention and preparation	2
Identifying data breaches.....	3
Reporting a data breach.....	3
Responding to a data breach	4
Containing a data breach	4
Assessing a data breach	5
Notification of an eligible data breach.....	6
Mandatory Notification of Data Breach Scheme under the <i>Privacy and Personal Information Protection Act 1998</i> (NSW)	7
Exemptions from certain requirements for an eligible data breach under the <i>Privacy and Personal Information Protection Act 1998</i> (NSW)	8
Post data breach review and evaluation.....	10
Records management	10
Section 4. Responsibilities	10
Section 5. Governance information	11
Section 6. Definitions	12
Section 7. Document history	13

Section 1. Purpose

- 1.1 This policy outlines the principles and procedure for responding to a data breach involving personal information or health information held by TAFE NSW, including notification requirements under the:
 - a. NSW Mandatory Notification of Data Breach Scheme; and
 - b. Commonwealth Notifiable Data Breaches Scheme (where applicable).
- 1.2 This policy also supports TAFE NSW compliance with:
 - a. [Privacy and Personal Information Protection Act 1998 \(NSW\)](#) (PIIP Act);
 - b. [Health Records and Information Protection Act 2002 \(NSW\)](#) (HRIP Act);
 - c. [Privacy Act 1988 \(Cth\)](#) (where applicable); and
 - d. other relevant legal and regulatory requirements.

Section 2. Scope

- 2.1 This policy applies to:
 - a. all TAFE NSW staff and all other relevant parties (including visitors, contractors and suppliers) who collect, manage, store, access or use any data that involves personal information or health information on behalf of TAFE NSW; and
 - b. actual and suspected data breaches involving personal information or health information.

Section 3. Policy statements

- 3.1 TAFE NSW is committed to protecting the personal information and health information it holds and managing data breaches in a timely and effective way. In managing the risks associated with data breaches, TAFE NSW will take reasonable steps to:
 - a. prevent data breaches;
 - b. identify and respond promptly to suspected or actual data breaches including taking immediate steps to contain the breach, where practicable, and escalating incidents in accordance with this Policy;
 - c. assess the risks arising from data breaches;
 - d. contain data breaches and mitigate harm to affected individuals and TAFE NSW;
 - e. follow all applicable notification and reporting requirements;
 - f. learn from incidents and continually improve information handling practices; and
 - g. promote a culture of privacy, accountability and information stewardship.
- 3.2 For the purposes of this policy, personal information includes health information.

Data breach prevention and preparation

- 3.3 TAFE NSW maintains a range of privacy, information security and governance controls to prevent, identify and respond to data breaches. These measures include:

- a. privacy impact assessments and security risk assessments;
- b. records management controls;
- c. contractual requirements for service providers;
- d. access controls, security monitoring and testing;
- e. secure information handling practices;
- f. staff education and awareness activities; and
- g. the secure destruction of records in accordance with legal requirements and relevant TAFE NSW policies and procedures.

3.4 For more information, refer to TAFE NSW's [Privacy Policy](#) and [Privacy Management Plan](#).

Identifying data breaches

3.5 A data breach occurs when personal information that is held by TAFE NSW is subject to unauthorised access, unauthorised disclosure or is lost in circumstances where the loss is likely to result in unauthorised access or unauthorised disclosure. A data breach can be suspected or known.

3.6 A data breach may occur in situations where, for example:

- a. user credentials are exposed, resulting in unauthorised access to or removal of personal information from TAFE NSW systems;
- b. personal information is emailed to the wrong recipient;
- c. personal information is not handled or stored in accordance with the correct security classification or with the required security or access controls;
- d. there is a failure to comply with TAFE NSW's [Privacy Policy](#), [Privacy Management Plan](#) and/or [Records Management Policy](#);
- e. a portable device or physical record is lost in a public or unsecured place;
- f. artificial intelligence applications are used without the correct approvals;
- g. personal information is accessed by external actors through a cyberattack, or
- h. someone's legitimate access to information is misused.

Reporting a data breach

3.7 Any TAFE NSW staff member or third-party contractor/supplier who becomes aware of, or is notified of, a suspected or actual data breach relating to personal information held by TAFE NSW, must report it immediately via email to itsecurity@tafensw.edu.au.

3.8 Third party contractors/suppliers should contact TAFE NSW via the IT Service Desk (1300 823 343) before reporting a data breach by email. Where this is not practicable (e.g. outside of IT Service Desk hours of operation of 8am to 6pm), data breaches must still be reported via email as soon as possible to enable TAFE NSW to take prompt action.

3.9 Where possible, the report must include information about the date and time that the data breach was first discovered, the date and time that the breach occurred, the type of information involved, and the cause and extent of the breach. TAFE NSW may require additional information to be provided depending on the circumstances.

Responding to a data breach

- 3.10 When a data breach is identified, the Privacy Officer or Cyber Security Team (in collaboration with the Privacy Officer), will be responsible for managing, reporting and responding to the data breach. The data breach will be managed in accordance with the following process:
- Step 1: Contain the data breach to prevent any further compromise of personal information.
 - Step 2: Assess the risks associated with the data breach by investigating the breach.
 - Step 3: Notify affected individuals and any other third parties that need to be notified, including reporting eligible data breaches to the NSW Privacy Commissioner and any other applicable regulatory authorities.
 - Step 4: Review the data breach and response to identify longer-term action to prevent future breaches and improve how they are managed.
- 3.11 Where appropriate, the Privacy Officer and/or Cyber Security team will establish a Data Breach Response Team. The Data Breach Response Team will be led by the Privacy Officer, or a delegate appointed by the Privacy Officer. The membership of the Data Breach Response Team will depend on the nature and seriousness of the data breach and may include representatives from one or more of the following areas:
- Project Manager - to coordinate the team's activities.
 - Privacy Officer - to provide privacy expertise and breach handling experience.
 - Information Security and IT Support - for technical expertise and to support investigations involving ICT systems.
 - Legal support - to identify legal obligations and provide advice.
 - Representative from the affected business area - to provide operational information and advice.
 - People Group - to provide human resources advice and support where the data breach involves the actions of a staff member.
 - Communications - to assist with the communication strategy to affected individuals, the media and external stakeholders, including advice and communication resources.
- 3.12 Where appropriate, the Data Breach Response Team may engage an external third party to assist in investigating and/or assessing the data breach.
- 3.13 Where a data breach involves data from another agency or third party, the Privacy Officer will advise and consult with the relevant party regarding the responsibilities and steps needed to respond to the breach.

Containing a data breach

- 3.14 Appropriate action must be taken as soon as possible to contain the data breach or limit its impact (i.e. TAFE NSW must make all reasonable attempts to mitigate any actual or potential harm caused by the breach).
- 3.15 Once a data breach is reported, the Privacy Officer and/or Cyber Security Team will manage the response to contain the data breach.

- 3.16 To assist with containing a data breach, staff who identify or become aware of a data breach should, where possible and within the scope of their role, take reasonable early action to support containment.
- 3.17 The action taken to contain the data breach will depend on the nature of the breach and the circumstances. For example, it may include stopping the unauthorised practice, recalling an email, recovering the records, shutting down the system that was breached or changing access.

Assessing a data breach

- 3.18 The Data Breach Response Team, under the leadership of the Privacy Officer and Cyber Security Team (as applicable), will investigate and assess the data breach as soon as possible (an assessment). The assessment will consider any associated risks (such as the risk of harm to affected individuals as a result of the breach), and will determine whether the breach is an eligible data breach that is notifiable under either the [PPIP Act](#) or the [Privacy Act 1988 \(Cth\)](#).
- 3.19 The Data Breach Response Team must take all reasonable steps to complete the assessment within 30 days of TAFE NSW becoming aware of the data breach.
- 3.20 **Extension of assessment period**
- 3.20.1 If the Privacy Officer determines that the assessment cannot reasonably be completed within 30 days, they may approve an extension for the period reasonably required to complete the assessment.
- 3.20.2 If an extension is approved, the Privacy Officer must do the following within the initial 30-day period:
- ensure that the assessment has commenced; and
 - notify the NSW Privacy Commissioner in writing that the assessment has commenced, an extension has been approved, and the length of the approved extension.
- 3.20.3 If the assessment is not completed within the extension period, the Privacy Officer must notify the NSW Privacy Commissioner in writing before the end of the extension period that:
- the assessment is ongoing;
 - a further extension has been approved by the Privacy Officer; and
 - the length of the approved further extension period.
- 3.21 When assessing the risks associated with a data breach, the Privacy Officer, Cyber Security Team and/or Data Breach Response Team will consider a range of factors, including but not limited to:
- the type, sensitivity and volume of personal information involved in the data breach;
 - the circumstances of the data breach, including its cause and extent;
 - whether the personal information is or was protected by security measures;
 - the persons involved in the data breach, including the likelihood that they intended to cause harm or circumvent security measures protecting the information; and
 - the nature and severity of the potential harm to affected individuals, including the likelihood of that harm eventuating.

- 3.22 TAFE NSW must also consider any other factors outlined in any guidelines issued by the NSW Privacy Commissioner, including factors that may reduce the risk of harm (e.g. such as preventative measures and attempts to mitigate any potential harm by TAFE NSW).
- 3.23 TAFE NSW takes a cautious approach to managing risk relating to information security and privacy, particularly in cases where information about a suspected data breach might be unclear or unknown. An assessment of risk may be higher in cases where, for example:
- the personal information is more sensitive in nature;
 - the data breach involves a large amount of personal information; or
 - details about the breach and associated risks cannot be confirmed (e.g. personal information has been made available online but it is not clear who has accessed it).
- 3.24 Following an assessment, the Privacy Officer will decide:
- whether there has been a data breach; and
 - if there has been a data breach, whether it is an eligible data breach under either the [PPIP Act](#) or the [Privacy Act 1988 \(Cth\)](#) or there are reasonable grounds to believe it is an eligible data breach.

Notification of an eligible data breach

- 3.25 Where the Privacy Officer determines on reasonable grounds that an eligible data breach has occurred, the Privacy Officer will:
- immediately notify the Managing Director;
 - immediately notify the NSW Privacy Commissioner in accordance with the Mandatory Notification of Data Breach Scheme, as outlined in section 3.28 below; and
 - as soon as practicable, notify the Australian Information Commissioner if a data breach involves tax file numbers that TAFE NSW holds or other personal information where TAFE NSW is subject to the [Privacy Act 1988 \(Cth\)](#).
- 3.26 The Data Breach Response Team will also determine if it is appropriate and necessary to notify any other third parties, having regard to any other legal and contractual obligations that require TAFE NSW to notify them, including applicable foreign data protection/privacy laws. This may include but is not limited to:
- the Australian Cyber Security Centre (approved and undertaken by the Cyber Security Team);
 - the Police;
 - insurance providers;
 - credit card companies and/or financial institutions;
 - professional or other regulatory bodies;
 - other third-party organisations or Government agencies whose data may be affected or as otherwise required by law or contract; and/or
 - any other parties that must be notified under applicable foreign data protection or privacy laws.
- 3.27 TAFE NSW may rely on any applicable exemption available under legislation where TAFE NSW determines it is appropriate to do so in the circumstances.

Mandatory Notification of Data Breach Scheme under the [Privacy and Personal Information Protection Act 1998 \(NSW\)](#)

Notification to the NSW Privacy Commissioner

- 3.28 If the Privacy Officer determines on reasonable grounds that an eligible data breach has occurred, the Privacy Officer will immediately notify the NSW Privacy Commissioner using the approved form (as issued by the NSW Privacy Commissioner).

Notification to individuals

- 3.29 As soon as practicable after determining that an eligible data breach has occurred, TAFE NSW must, to the extent that it is reasonably practicable, notify:
- a. each individual to whom the personal information the subject of the data breach relates; or
 - b. each affected individual,
- unless an applicable exemption applies under Part 6A, Division 4 of the [PPIP Act](#).
- 3.30 The Privacy Officer will determine who from TAFE NSW will make the notification to affected individuals.
- 3.31 In addition to any obligations under law or contract, TAFE NSW should notify affected individuals if the Privacy Officer determines that there is a foreseeable risk of harm to an affected individual as a result of the data breach.
- 3.32 Affected individuals under this policy will be notified using the relevant primary communication method for that individual (e.g. via student or staff email accounts or by letter or phone as appropriate). TAFE NSW may use alternative notification methods where appropriate on a case-by-case basis, having regard to the nature of the data breach and needs of affected individuals (e.g. TAFE NSW may also choose to meet with students personally).
- 3.33 A notification to individuals must, if reasonably practicable, include the following information:
- a. the date the data breach occurred;
 - b. a description of the data breach;
 - c. how the data breach occurred;
 - d. the type of data breach that occurred (e.g. unauthorised disclosure, unauthorised access, loss of information);
 - e. the personal information that was the subject of the data breach;
 - f. the amount of time the personal information was disclosed for;
 - g. actions that have been taken or are planned to ensure the personal information is secure, or to control or mitigate the harm done to the individual;
 - h. recommendations about the steps the affected individual should take in response to the breach;
 - i. information about how to make a privacy related complaint and seek an internal review; and
 - j. the name of TAFE NSW if it was the subject of the breach, and the name of any other public sector agencies who were the subject of the breach, including contact details for TAFE NSW and each other agency.

- 3.34 If some information is not available (e.g. in more complex matters), it may be appropriate to provide information to individuals in stages to avoid undue delay in notification, as more information becomes available.
- 3.35 Where affected individuals are also current TAFE NSW staff, they may access staff support services including Employee Assistance Program (EAP).

Public notification register

- 3.36 TAFE NSW must maintain a public notification register on its website. TAFE NSW will publish a notification of any eligible data breaches on the public notification register where:
- TAFE NSW is unable to notify, or it is not reasonably practicable to notify, any or all the affected individuals; or
 - the Privacy Officer otherwise decides TAFE NSW should issue a public notification.
- 3.37 When publishing a notification on the public notification register, TAFE NSW must:
- keep the notification on the register for at least 12 months; and
 - include the information specified in section 3.33 above, where reasonably practicable, except to the extent that the information contains personal information or its publication would prejudice TAFE NSW functions.
- 3.38 As soon as practicable after the notification is published, the Privacy Officer must provide the NSW Privacy Commissioner with information about how to access the notification and public notification register.

Exemptions from certain requirements for an eligible data breach under the [Privacy and Personal Information Protection Act 1998 \(NSW\)](#)

- 3.39 TAFE NSW is not required to notify affected individuals of an eligible data breach if any of the exemptions in Part 6A, Division 4 of the [PPIP Act](#) apply (as outlined below). These exemptions may not apply to the extent that other privacy and foreign data protection or privacy legislation applies.

Exemption for eligible data breaches of multiple public sector agencies

- 3.40 If an eligible data breach involves other public sector agencies (in addition to TAFE NSW) and the other agency involved undertakes to notify affected individuals and the NSW Privacy Commissioner, TAFE NSW is not required to notify affected individuals or make any public notification.

Exemption for ongoing investigations and certain proceedings

- 3.41 TAFE NSW is not required to notify affected individuals or make any public notification if the Privacy Officer reasonably believes notification of an eligible data breach would be likely to prejudice:
- an investigation that could lead to the prosecution of an offence;
 - proceedings before a court or a tribunal; or
 - another matter prescribed under the applicable regulations for the purpose of this section.

Exemption if TAFE NSW has taken certain action

3.42 If an eligible data breach involves:

- a. unauthorised access to, or disclosure of, personal information held by TAFE NSW;
- b. TAFE NSW takes action to mitigate the harm done by the breach before the access to, or disclosure of, information results in serious harm to an individual; and
- c. a reasonable person would conclude that the access or disclosure would not likely result in any serious harm to an individual;

TAFE NSW is not required to notify affected individuals or make any public notification.

3.43 If an eligible data breach involves:

- a. loss of personal information held by TAFE NSW;
- b. TAFE NSW takes action to mitigate the loss before there is unauthorised access to, or disclosure of, the information; and
- c. because of the action taken there is no unauthorised access to, or disclosure of, the information;

TAFE NSW is not required to notify affected individuals or make any public notification.

Exemption if inconsistent with secrecy provisions

3.44 If notification of an eligible data breach would be inconsistent with another legislative act or statutory rule that prohibits or regulates the use or disclosure of information, TAFE NSW is not required to notify affected individuals or make any public notification.

Exemption if serious risk of harm to health and safety

3.45 If the Privacy Officer reasonably believes that notification would create a serious risk of harm to an individual's health or safety, TAFE NSW is not required to notify affected individuals.

3.46 In making this decision, the Privacy Officer will:

- a. consider the extent to which the harm of notifying the eligible data breach is greater than the harm of not notifying the breach;
- b. consider the currency of the information relied on in assessing the serious risk of harm to an individual; and
- c. not search, require or permit the search of data held by TAFE NSW, that was not affected by the breach, to assess the impact of notification, unless the Privacy Officer knows, or reasonably believes, that the data contains information relevant to the application of this section.

3.47 The Privacy Officer must also notify the NSW Privacy Commissioner in writing when TAFE NSW relies on this exemption under section 59W of the [PPIP Act](#), including whether the exemption is permanent or temporary and, if temporary, the specified or expected time that the exemption will be relied on.

Exemption for compromised cyber security

3.48 If the Privacy Officer reasonably believes that notification would worsen TAFE NSW's cyber security or lead to further data breaches, TAFE NSW is not required to notify affected individuals.

- 3.49 When TAFE NSW relies on an exemption due to compromised cyber security for a period of time, the Privacy Officer must notify the NSW Privacy Commissioner in writing and include:
- when the exemption is expected to end; and
 - the way TAFE NSW will review its continued application.
- 3.50 The Privacy Officer must also review the use of the exemption each month and provide an update to the NSW Privacy Commissioner on the review of the exemption.

Post data breach review and evaluation

- 3.51 The Privacy Officer, with the support of the Data Breach Response Team, will conduct a post data breach review and evaluation to:
- identify any weaknesses in the processes, systems or activities that may have contributed to the data breach;
 - assess the effectiveness of TAFE NSW's data breach response activities under this policy;
 - develop a proposed action plan for any identified preventative measures and mitigation strategies to implement; and
 - propose relevant updates to the Privacy Management Plan and this policy.

Records management

- 3.52 Any records created in relation to a data breach will be managed in accordance with TAFE NSW's [Records Management Policy](#).

Section 4. Responsibilities

Position, Branch or Unit	Responsibilities
Cyber Security Team	Responsible for managing and responding to a data breach, in collaboration with the Privacy Officer, where applicable e.g. where the data breach involves TAFE NSW ICT systems or equipment.
Data Breach Response Team	TAFE NSW personnel who are appointed and responsible for assessing and managing a data breach. The membership of the data breach response team will depend on the nature and seriousness of the data breach but will at least include the Privacy Officer and a delegate from the Cyber Security team where applicable (e.g. where the breach involves TAFE NSW ICT systems or equipment).

Privacy Officer	Responsible for managing and responding to a data breach including by: • leading the Data Breach Response Team (or appointing a delegate to lead as appropriate); • providing advice to other staff on how to respond to a data breach, including advice on containment and mitigation; • assessing whether a data breach is an 'eligible data breach'; • determining notification requirements in relation to any 'eligible data breach'; • notifying relevant regulators where required; • maintaining oversight of data breach management activities.
All TAFE NSW staff	All staff are responsible for: • complying with this policy and related procedures; • immediately reporting suspected or actual personal data breaches; • participating in training as required.
Line managers, senior and executive leadership	All managers and senior leadership are responsible for: • promoting compliance with this policy and related procedures; • ensuring staff complete mandatory privacy and information security training; • supporting investigations and remediation activities; • ensuring suspected breaches are escalated promptly
Contractors, suppliers and service providers	Protect personal information held on behalf of TAFE NSW, comply with contractual privacy requirements, and promptly report actual or suspected data breaches involving TAFE NSW information.

Section 5. Governance information

Governance	Details
Legislation, regulations, and standards	This procedure is governed by: • Privacy and Personal Information Protection Act 1998 (NSW) • Health Records and Information Protection Act 2002 (NSW) • Privacy Act 1988 (Cth) • State Records Act 1998 (NSW)

Associated policies and procedures	This policy is to be read together with: • Privacy Policy • Privacy Management Plan • Data Governance Policy • Information Security Policy • Acceptable Use of Information and Technology Policy • Records Management Policy
Accountable Officer	Chief Operating Officer
Responsible Officer	Executive Director Governance Legal and Risk and General Counsel
Content Manager number	PROJ26/00410
Next review date	28 September 2029

Section 6. Definitions

Word	Definition
Data breach	a data breach occurs when personal information held by TAFE NSW is subject to unauthorised access, unauthorised disclosure or is lost in circumstances where the loss is likely to result in unauthorised access or unauthorised disclosure.
Eligible data breach	is defined in section 59D of the Privacy and Personal Information Protection Act 1998 (NSW) and means: - there is unauthorised access to, or unauthorised disclosure of, personal information held by TAFE NSW and a reasonable person would conclude that the access or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates; or - personal information held by TAFE NSW is lost in circumstances where: - unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and - if the unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to an individual to whom the information relates.
Health information	is defined in section 6 of the Health Records and Information Privacy Act 2002 (NSW) and means information or an opinion about: - the physical or mental health or a disability (at any time) of an individual; - an individual's express wishes about the future provision of health services to him or her; or - a health service provided, or to be provided, to an individual.

Commonwealth Notifiable Data Breach (NDB) Scheme	means the mandatory data breach notification scheme established under the Privacy Act 1988 (Cth) , which requires covered entities to notify the Office of the Australian Information Commissioner and affected individuals when an eligible data breach is likely to result in serious harm.
Mandatory Notification of Data Breach (MNDB) scheme.	means the NSW Mandatory Notification of Data Breach Scheme established under Part 6A of the Privacy and Personal Information Protection Act 1998 (NSW) , which requires NSW public sector agencies to assess, manage and notify eligible data breaches to affected individuals and the NSW Privacy Commissioner.
Personal Information	is defined in section 4 of the Privacy and Personal Information Protection Act 1998 (NSW) and means information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can be reasonably ascertained from the information or opinion. Unless otherwise specified, Personal information includes health information as defined in section 6 of the Health Records and Information Privacy Act 2002 (NSW)
Privacy Laws	means: • Privacy and Personal Information Protection Act 1998 (NSW); • Health Records and Information Protection Act 2002 (NSW) (HRIP Act); • Privacy Act 1988 (Cth) (where applicable); and • any other applicable data protection / privacy laws, including the European Union's General Data Protection Regulation (GDPR) and China's Personal Information Protection Law (PIPL).
Privacy Officer	means TAFE NSW's nominated privacy officer or their delegate.
Staff	means any person working in a casual, temporary or permanent capacity at TAFE NSW, including individual consultants and contractors.

Section 7. Document history

No.	Effective	Approved by	Amendment
1	28 September 2026	Managing Director	New policy developed based on existing content previously operationalised via the: • Privacy Management Plan (published version June 2023, clauses 2.7-2.7.7); and • Personal Data Breach Management Procedure (rescinded).