PRIVACY MANAGEMENT PLAN

TAFENSW.EDU.AU

INDEX

1. Introduction 3
1.1 Executive Summary 3
1.2 Scope 3
1.3 Privacy laws 3

2. Managing Privacy 4
2.1 Collection of personal information 4
2.2 Storage and security of personal information 8
2.3 Access to information 9
2.4 Using personal information 10
2.5 Disclosing personal information 11
2.6 General privacy exemptions 13
2.7 Managing data breaches 14

3. Country-specific data protection laws 18

4. Complaints 19
4.1 Making a complaint 19
4.2 Privacy internal review 19

5. Education and Training 21
5.1 Policy and governance 21
5.2 Privacy Impact Assessments 21
5.3 Education and training 21

6. Plan updates 21

APPENDIX 1 - Definitions 22

1. Introduction

1.1 Executive Summary

The Technical and Further Education Commission (**TAFE NSW**) is a statutory body established and operating under the *Technical and Further Education Commission Act 1990* (NSW) that provides technical and further education and training services.

As a leading provider of technical and further education and training services in Australia, TAFE NSW is committed to complying with all applicable data protection / privacy laws. As TAFE NSW's services extend internationally, its data privacy compliance program is built on a global centric foundation.

1.2 Scope

This Privacy Management Plan (**Plan**) has been developed in accordance with section 33 of the *Privacy and Personal Information Protection Act (NSW) 1998* (**PPIPA**) and applies to all personal and health information held by TAFE NSW and its controlled entities (if any).

The Plan details how TAFE NSW manages such personal and health information, and is a supporting document to the TAFE NSW Privacy Policy. The Plan also considers, where applicable, the requirements of the *Privacy Act 1988* (Cth) and country-specific data protection / privacy laws where TAFE NSW operates in country-specific jurisdictions or offers goods or services to citizens / residents in such jurisdictions.

1.3 Privacy laws

1.3.1 TAFE NSW is primarily governed by NSW privacy legislation, being the *Privacy and Personal Information Protection Act 1998* (NSW) (**PPIP Act**) and *Health Records and Information Protection Act 2002* (NSW) (**HRIP Act**).

1.3.2 TAFE NSW is also subject to the *Privacy Act 1988* (Cth), but only to the extent that TAFE NSW collects and holds any:

- personal information regarding student assistance provided by the Commonwealth, including under the *Higher Education Support Act 2003* (Cth)); and/or
- tax file numbers.

1.3.3 Where applicable, TAFE NSW may also be subject to other privacy and data protection legislation, including but not limited to, the European Union *General Data Protection Regulation* (**GDPR**) and China's *Personal Information Protection Law* (**PIPL**).

2. Managing Privacy

2.1 Collection of personal information

2.1.1 Personal information collected and held by TAFE NSW

TAFE NSW collects and holds personal and health information to support its functions related to education and training, research, student administration, student services and activities, complaints and disciplinary activities, recruitment and employment activities, health and well-being activities, employment and relationships with external parties. Examples of personal information that TAFE NSW may collect and hold, if permitted under applicable Privacy Laws, includes the following:

Students	Staff	Other parties
• Personal identifiers and contact information (e.g. name, student identification number, address, date of birth, gender and citizenship information) • Enrolment information • Digital photos for student identification cards • Financial information (e.g. tax file numbers, information relating to student loans, credit card details) • Educational and employment information (e.g. previous educational information, assessments, academic results, employment history) • Survey information • Background checks (e.g. working with children checks)	• Personal identifiers and contact information (e.g. name, staff identification numbers, address, date of birth, gender, and citizenship status) • Recruitment information, including background and security checks (e.g. police checks and working with children checks) • Digital photos for staff identification cards • Financial information (e.g. tax file numbers, banking details, remuneration details, superannuation details) • Educational employment and training information • Performance and career development information (e.g. performance reviews, work plans, assessment reports and information relating to grievances, complaints and misconduct) • Survey information • Staff communications	• Personal identifiers and contact information (e.g. name and contact details) of individuals associated with TAFE NSW, such as alumni and donors, volunteers, consultants, contractors, suppliers, industry partners, community groups and users of TAFE NSW facilities and systems

Examples of health information that TAFE NSW may collect and hold, if permitted under applicable Privacy Laws, includes the following:

As educational institution	As a service provider	As an employer
• Student welfare information (e.g. health and medical information, disability and equity information) • Medical records of students receiving counselling)	• Medical and health records of children attending TAFE NSW child-care centres • Medical records of persons receiving counselling or other clinical services	• Staff welfare and human resource information (e.g. health and medical information related to employment such as sick leave, workers compensation and occupational, health and safety information, disability and equity information)

2.1.2 Purposes for which personal information may be collected

TAFE NSW will only collect personal and health information by lawful means, for a lawful purpose, directly related to a function or activity of TAFE NSW, and which is reasonably necessary for that purpose in accordance with applicable Privacy Laws. These purposes may include:

- teaching and learning;
- the management of students, including recruitment, enrolment, academic progression and completion, accommodation, scholarships, assessment, complaints, disciplinary matters, services and support, conferral of awards, certificates and statements of attainment, and health, safety and wellbeing;
- the management of staff, including recruitment, retention, workforce planning, training and development, performance, remuneration, complaints, disciplinary matters, safety management, and health, safety and wellbeing;
- community engagement, including with community groups, student alumni, donors, sponsors, other educational organisations, industry and government;
- administrative functions, including management of monies and funds, security and safety of property and persons and managing the use of TAFE NSW property, facilities and equipment;
- research;
- provision of counselling, disability support and other services and support;
- commercial dealings that support the functions of TAFE NSW; and
- marketing and promoting TAFE NSW courses, services and events, including conducting surveys and competitions.

2.1.3 Collecting personal information directly from the individual

(a) TAFE NSW will only collect personal information directly from the individual to whom the information relates, unless:

- the individual provides consent for the information to be collected from another party;
- or the collection from another party is required or permitted by law;
- in the case of health information, it is unreasonable or impracticable to do so; or

- a specific exemption applies under applicable Privacy Laws.

In the case of information relating to a person who is under the age of 16 years, the information can be collected from a parent or legal guardian of that person.

(b) Another party may obtain the individual's consent that allows that party to provide the individual's personal information to TAFE NSW.

2.1.4 Collecting personal information from third parties

(a) TAFE NSW may also collect personal information from third parties, including:

- schools and other education and training providers;
- government agencies and departments;
- other organisations where TAFE NSW students undertake work placements or experience;
- employers;
- recruitment and employment agents; and
- parents or legal guardians of a minor who is enrolling or enrolled at TAFE NSW.

(b) Personal information may also be collected from other parties as part of investigations or proceedings carried out under applicable legislation, TAFE NSW policies and procedures or other instruments.

2.1.5 Collecting personal information through automated processes

TAFE NSW may also collect personal information through various automated processes, including:

- CCTV / security cameras located across all TAFE NSW campuses;
- video / audio recordings used for teaching, educational and training purposes e.g. recorded course delivery, or for staff training and development purposes, as well as through recorded meetings conducted via online platforms such as Microsoft Teams or Zoom;
- collecting information about visits to TAFE NSW websites for security and quality improvement purposes using web analytics and cookies;
- logging users of the TAFE NSW WiFi service and information management systems and equipment to facilitate and monitor use; and
- logging staff and student access to TAFE NSW facilities such as building and rooms using swipe cards.

2.1.6 Open collection of personal information

(a) When collecting personal information directly from an individual, TAFE NSW will take reasonable steps to ensure that, before the information is collected or as soon as practicable after collection, the individual is made aware of the following information:

- the fact that the information is being collected;
- the purpose for which the information is being collected and how it will be used;
- whether the information will be disclosed, and if so, to whom and for what reason;

- whether the supply of the information is voluntary or required by law, and any consequences if the information is not provided;
- how an individual can request access to the information or amend / update it; and
- relevant contact details for an individual to direct requests or questions regarding their privacy.

(b) In some circumstances, it may also be necessary to inform individuals of the following additional information, particularly if an activity is covered by GDPR:

- identifying the lawful grounds that allows TAFE NSW to process the information;
- additional rights of the individual, including the right to request transfer/data portability, data deletion/erasure, object to or restrict processing, and where to lodge a privacy complaint;
- if information will be transferred to another country, including if information will be transferred or stored outside of Australia, or outside where it originated from in the European Union;
- if there is any automated decision-making processes involved in the activity, and how they operate (if applicable); and
- how long the information will be kept, or alternatively how retention will be determined.

(c) TAFE NSW will inform individuals of the above information through its privacy collection notices and statements as required; and will ensure that the privacy notice or statement is in clear and plain language, easily accessible and clearly distinguishable from any other information being provided, to ensure that the individual has understood and provided informed consent.

(d) TAFE NSW will provide a privacy notice or statement in a variety of ways, including:

- on a form that collects personal information;
- on a consent form;
- on a web page;
- in the terms and conditions for an application, information system or other service; and/or
- in a policy or procedure document, such as TAFE NSW's Privacy Policy.

2.1.7 Relevant and lawful collection of personal information

(a) When collecting personal information directly from an individual, TAFE NSW will take reasonable steps to ensure that the information collected:

- is relevant, accurate, up-to-date and complete, and is not excessive; and
- does not unreasonably intrude on the personal affairs of the individual.

(b) Whether information collected is relevant and necessary will depend on why the information is being collected.

(c) TAFE NSW will only collect personal information for a lawful purpose, and where it is necessary for and directly relates to TAFE NSW's activities. The lawful

bases under which TAFE NSW may collect and process personal information include:

- *consent* - the individual has given consent for TAFE NSW to process their personal information for one or more processing activities;
- *contract* - the processing activity is necessary to enter into or perform a contract with the individual;
- *legitimate interest* – the processing is necessary for TAFE NSW's legitimate interests or the legitimate interests of a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual which requires protection of their personal information;
- *vital interests* – the processing is necessary to protect a person's vital interests (e.g. someone's life in a medical emergency situation);
- *legal obligation* – the processing activity is necessary for TAFE NSW to comply with a legal obligation to which TAFE NSW is subject; and
- *public interest* - the processing activity is necessary for TAFE NSW to perform a task in the public interest or for its official functions.

2.2 Storage and security of personal information

2.2.1 Storage and Security

(a) The security of personal information held by TAFE NSW is of the utmost importance. TAFE NSW will take such security safeguards as are reasonable to protect personal information from unauthorised access, alteration, use and disclosure. TAFE NSW will also store personal information securely and keep it no longer than necessary, and will dispose of it securely.

(b) TAFE NSW protects personal information through a combination of technical security measures and practices, including:

- having appropriate policies and procedures in place, including policies and procedures relating to access, use and disclosure of personal information;
- conducting privacy impact assessments to identify and mitigate any privacy risks to personal information;
- conducting security impact assessments to ensure that appropriate security measures and controls are in place to protect personal information;
- having record management systems which govern the storage, access, retention and destruction of records in accordance with TAFE NSW's obligations under the *State Records Act 1998* (NSW) and other applicable legislation;
- having enforceable contracts with service providers / vendors that host systems and data, or collect, store and/or process information on behalf of TAFE NSW;
- protection of information systems and data through passwords, security testing and monitoring and implementation of user rights and access controls;
- securely storing, transporting and destroying paper and digital records, including digital storage devices containing personal information; and

- staff education and training programs.

2.2.2 Destruction

(a) TAFE NSW records, including those containing personal information, will be destroyed using appropriate destruction methods in accordance with TAFE NSW's obligations under applicable legislation, including the *State Records Act 1998* (NSW), and TAFE NSW policies and procedures.

Requests for destruction / erasure

(b) Under the GDPR and the PIPL, some individuals have the right to request that their personal information held by TAFE NSW is permanently erased or deleted. If an eligible individual makes such a request under that legislation, the personal information of that individual will only be erased or deleted subject to TAFE NSW's obligations under the *State Records Act 1998* (NSW) and any other applicable legislation which requires TAFE NSW to retain it.

2.3 Access to information

2.3.1 Access to personal information

(a) TAFE NSW will take reasonable steps to enable an individual to know whether TAFE NSW holds personal information about them, and if so:

- the nature of that information;
- the main purpose for which the information is used; and
- their right to access the information.

This information may be provided on request and/or included in a relevant privacy notice or statement.

(b) Where an individual requests access to their personal information held by TAFE NSW, the request will be actioned without excessive delay or expense. The volume and nature of personal information requested will affect how long the request will take to action.

(c) Individuals seeking information about whether TAFE NSW holds their personal information, or who wish to access their personal information, should contact TAFE NSW as follows:

- **TAFE NSW students** can access their contact details and other information related to their enrolment through My LEARNER PORTAL (which can be accessed via my.tafensw.edu.au) or by contacting Student Services on 131 601 or via the Student Services webpage.
- **TAFE NSW staff** can access their personal information through the People@TAFE application (which can be accessed via the staff portal).
- **TAFE NSW counselling clients** can access their medical records and personal information held by TAFE NSW by contacting the relevant area in the first instance.
- **Other individuals** can access their personal information by contacting the relevant area within TAFE NSW that they normally interact with.

(d) If access to an individual's personal information is not provided on initial request, they can:
- send a formal request (made under PPIPA or HRIPA) to the TAFE NSW Privacy Officer at privacy@tafensw,edu.au; or
- lodge an access application under *the Government Information (Public Access) Act 2009* (NSW) (**GIPA Act**).

(e) In most cases access will be provided at no cost to the individual, except where:
- information is available for purchase (e.g. production of transcripts, testamurs and certificates / statements of course completion);
- access is requested to health information; and
- access is requested under the GIPA Act.

(f) When dealing with an individual about their personal information. TAFE NSW may require the individual to verify their identity to ensure that TAFE NSW is dealing with the right person.

(g) In some cases, certain information may not be released until outstanding debts have been paid (e.g. a student's results may be withheld if they have any outstanding course fees that have not be paid). In some cases, a request to access information may be refused by TAFE NSW (e.g. where permitted or required by law).

2.3.2 Amending personal information

(a) Where necessary individuals can update, correct or amend their personal information held by TAFE NSW through the same process used to access personal information as specified in section 2.3.1(c) above.

(b) In some cases, certain changes (e.g. a change of name) may require the individual to provide supporting information as evidence. If TAFE NSW is not prepared to amend personal information as requested, TAFE NSW will, if requested by the individual, take reasonable steps to attach to the information a statement of the amendment that was sought.

2.4 Using personal information

2.4.1 Accuracy

(a) TAFE NSW will take reasonable steps to ensure that the personal information it holds is relevant, accurate, up-to-date, complete and not misleading before using it, having regard to the purpose(s) for which the information is to be used, including:
- enabling staff and students to access and update their personal information through available IT systems;
- providing email reminders to staff and students to keep their personal information up-to-date; and
- where practical, having one authoritative source of information that is maintained, rather than maintaining multiple sources of the same information.

(b) TAFE NSW will not use any personal information where it is known to contain incorrect information.

2.4.2 Using personal information

(a) TAFE NSW will only use personal information that it holds for the purpose(s) for which it was collected, unless:

- the individual to whom the personal information relates has consented to the use of the personal information for another purpose;
- the other purpose for which the information is to be used is directly related to the purpose for which the personal information was collected;
- the use of the personal information is necessary to lessen or prevent a serious and imminent threat to the life or health of any person;
- required or permitted by law;
- it is reasonably necessary for law enforcement purposes or for the protection of public revenue; or
- reasonably necessary to assist in an emergency situation.

(b) Other exemptions regarding use of personal information may also apply under applicable Privacy Laws. TAFE NSW may also use personal information it holds for administrative purposes, including:

- internal quality assurance, training and planning purposes; and
- managing complaints, investigations, claims or litigation.

(c) The general uses of personal information held by TAFE NSW are also set out in TAFE NSW's privacy collection notices and statements (including TAFE NSW's Privacy Policy) and consent forms.

Withdrawal of consent

(d) Where an individual has provided consent and later withdraws consent for their personal information to be used, TAFE NSW will take reasonable steps to comply with the request as soon as practically possible, subject to any requirements under the *State Records Act 1998* (NSW) and any other applicable legislation.

2.5 Disclosing personal information

2.5.1 When personal information may be disclosed

(a) TAFE NSW will not disclose personal information that it holds to any other person or body, unless:

- the disclosure is directly related to the purpose for which the personal information was collected, and TAFE NSW has no reason to believe that the individual concerned would object to the disclosure;
- the individual concerned is reasonably likely to have been made aware, or has been made aware when the personal information was collected, that personal information of that kind is usually disclosed to that other person or body;

- TAFE NSW reasonably believes that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of any person; or
- required or permitted by law.

Examples of when TAFE NSW may disclose personal information include but are not limited to:

- to government agencies and regulatory authorities where disclosure is required or permitted by law, or for mandatory reporting obligations (e.g. State education departments, Commonwealth education and immigration departments or the National Centre for Vocational Education Research)
- law enforcement agencies;
- to credit-reporting bodies and debt collection agencies;
- where information is requested under a valid subpoena, warrant or court order;
- where it is necessary for TAFE NSW to manage investigations or complaints, claims, litigation or insurance matters;
- other education and training providers that TAFE NSW works with to provide education and training; and
- to third parties who assist TAFE NSW in managing, marketing or developing its business, including products and services.

(b) Other exemptions regarding disclosure of personal information may also apply under applicable Privacy Laws.

(c) The general disclosure of personal information held by TAFE NSW is also set out in TAFE NSW's privacy collection notices and statements (including TAFE NSW's Privacy Policy) and consent forms.

Internal access to personal information

(d) Providing information to different business areas within TAFE NSW is not considered disclosure for the purpose of section 2.5.1 above. However, personal information should only be accessed by, or provided to, other TAFE NSW staff members who require the information for a legitimate purpose.

(e) All TAFE NSW staff must comply with the TAFE NSW 'Code of Conduct and Ethical Practices' and relevant policies and procedures governing appropriate access, use and disclosure of personal information.

2.5.2 Disclosing sensitive personal information

TAFE NSW will not disclose personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities, unless the disclosure is necessary to prevent a serious and imminent threat to the life or health of the individual concerned or any other person.

2.5.3 Disclosing personal information outside of NSW

(a) TAFE NSW will not disclose any personal information it holds outside of NSW or to a Commonwealth agency, unless:

- TAFE NSW reasonably believes that the recipient of the information is subject to a law, binding scheme or contract that effectively upholds privacy principles that are substantially similar to the IPPs or HPPs;
- the individual expressly consents to the disclosure;
- the disclosure is necessary for the performance of a contract (either between the individual and TAFE NSW or in the interests of the individual if the contract is between TAFE NSW and a third party);
- the disclosure is for the benefit of the individual and it is impracticable to obtain the consent of the individual to that disclosure, and the individual would otherwise be likely to give consent;
- disclosure is reasonably necessary to lessen or prevent a serious and imminent threat to the life, health or safety of the individual or any person;
- TAFE NSW has taken reasonable steps to ensure that the disclosed personal information will not be held, used or disclosed by the recipient inconsistently with the IPPs or HPPs; or
- required or permitted by law.

(b) If personal information is disclosed outside of Australia TAFE NSW will perform an appropriate transfer impact assessment in relation to the transfer of personal information to the relevant jurisdiction outside of Australia.

2.5.4 Additional requirements covering use and disclosure of health information

Information identifiers and anonymity

(a) TAFE NSW may use unique identifiers (e.g. identification numbers or other codes) if it is reasonably necessary to carry out TAFE NSW functions efficiently.

(b) TAFE NSW may provide health services anonymously where it is lawful and practicable to do so.

Linkage of health records

(c) TAFE NSW will not link an individual's health information in a health records linkage system with those of another organisation without the individual's express consent.

2.6 General privacy exemptions

Under applicable Privacy Laws, including the PPIP Act and HRIP Act, there are exemptions to certain privacy requirements. TAFE NSW will only rely on those exemptions where it is appropriate to do so in the circumstances.

2.6.1 Public interest directions

The NSW Privacy Commissioner may make public interest directions that modify the application of privacy principles in some circumstances. TAFE NSW will only apply public interest directions that are applicable in the circumstances.

2.6.2 Public registers

TAFE NSW will only make a public register available to the public where it is satisfied that it will only be used for a purpose relating to the purpose of the register or the law under which the register is kept.

2.6.3 Research

TAFE NSW may collect, use and disclose personal information for the purpose of research, or the compilation or analysis of statistics, in the public interest, without obtaining an individual's consent provided it complies with all applicable requirements specified in the PPIP Act and HRIP Act, any Statutory Guidelines issued by the NSW Privacy Commissioner and obtains approval from the Privacy Officer.

2.7 Managing data breaches

Although processes are in place to protect personal information TAFE NSW holds, if such information has been lost, or subject to unauthorised access, modification or disclosure, a data breach will have occurred and will be managed in accordance with this section, including TAFE NSW's Personal Data Breach Management Procedure and any applicable Privacy Laws.

2.7.1 Reporting a data breach

(a) Any TAFE NSW staff member who identifies, or is advised of, a suspected or known data breach must report it as soon as possible:

- if the data breach involves TAFE NSW ICT systems or equipment (e.g. is a cyber incident), it should be reported to the TAFE NSW Cyber Security team at itsecurity@tafensw.edu.au.
- all other data breaches should be reported to the Privacy Officer at privacy@tafensw.edu.au.

(b) Where possible the report should include information about the time and date that the data breach was first discovered, the type of information involved, and the cause and extent of the breach.

2.7.2 Containing a data breach

(a) Once a data breach has been identified, appropriate action must be taken to immediately contain it or limit the extent of the breach (i.e. TAFE NSW must make all reasonable attempts to mitigate the harm done by the breach). The action taken to contain the data breach will depend on the nature of the breach (e.g. it may include stopping the unauthorised practice, recovering the records, shutting down the system that was breached or changing access codes).

(b) The Privacy Officer may also be consulted in the first instance to obtain advice on how to deal with the data breach.

2.7.3 Assessing a data breach

(a) TAFE NSW will investigate and assess the data breach, and take all reasonable steps to ensure that the assessment is completed within 30 days after becoming aware of the breach. If the Privacy Officer is satisfied that an assessment cannot reasonably be conducted within 30 days, the Privacy Officer may approve an extension of the period as is reasonably required to complete the assessment.

(b) Some of the factors that will be considered when assessing risk include:

- 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 who were involved in the data breach, including the likelihood of them intending to cause harm or circumventing security measures protecting the information; and
- the nature and severity of the potential harm to the affected individuals, including the likelihood of such harm eventuating.

(c) TAFE NSW must also consider any other factors outlined in any guidelines issued by the NSW Privacy Commissioner, including any other factors that may reduce the risk of harm (e.g. such as preventative measures and attempts to mitigate any potential harm by TAFE NSW).

(d) Following an assessment, the Privacy Officer will decide whether the data breach is an eligible data breach or there are reasonable grounds to believe it is an eligible data breach.

2.7.4 Mandatory notification of eligible data breaches

(a) *Notification to the NSW Privacy Commissioner*

If the Privacy Officer determines on reasonable grounds that an eligible data breach has occurred, the Privacy Officer must immediately notify the NSW Privacy Commissioner of the breach using the approved form (as issued by the NSW Privacy Commissioner). The approved form will specify the type of information that must be provided in relation to the eligible data breach, unless:

(i) it is not reasonably practicable to provide the information, in which case the information must be provided following notification to the individuals specified in section 2.7.4(b) below; or

(ii) an exemption under section 2.7.5 below applies.

(b) *Notification to individuals*

As soon as practicable after the Privacy Officer decides that an eligible data breach has occurred, the Privacy Officer must, to the extent that it is reasonably practicable, notify:

- each individual to whom the personal information the subject of the breach relates; or
- each affected individual,

unless an exemption under section 2.7.5 below applies.

(c) A notification to individuals must, if it is reasonably practicable for the information to be provided, include certain specified information in relation to each eligible data breach, such as the date the breach occurred, a description of the breach, the type of breach and how it occurred, the personal information involved and amount of time it was disclosed for, proposed mitigation actions and recommendations for affected individuals, information on how to make a complaint and contact details of who to contact about the breach.

(d) *Public notification*

(i) If TAFE NSW is unable to notify, or if it not reasonably practicable for TAFE NSW to notify, any or all of the individuals specified in section 2.7.4(b) above, or the Privacy Officer otherwise decides to notify publicly under this section, TAFE NSW must:

- publish the notification on TAFE NSW's website via a register (a public notification register) for at least 12 months after the date the notification is published; and
- if it is reasonably practicable for the information to be provided, include the information specified in section 2.7.4(c) above, except to the extent it contains personal information or would prejudice TAFE NSW's functions.

(ii) 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 on the public notification register (e.g. a link to the TAFE NSW website on which the notification is published).

2.7.5 Exemptions from certain requirements for an eligible data breach

TAFE NSW is not required to notify affected individuals or make any public notification if any of the following exemptions apply:

(a) *Exemption for eligible data breaches of multiple public sector agencies*

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.

(b) *Exemption relating to ongoing investigations and certain proceedings*

If the Privacy Officer reasonably believes notification of the 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.

(c) *Exemption if TAFE NSW has taken certain action*

(i) If an eligible data breach involves unauthorised access to, or disclosure of, personal information held by TAFE NSW, and 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 a reasonable person would conclude that the access or disclosure would not likely result in any serious harm to an individual.

(ii) If an eligible data breach involves loss of personal information held by TAFE NSW, and TAFE NSW takes action to mitigate the loss before there is unauthorised access to, or disclosure of, the information and because of the action taken there is no unauthorised access to, or disclosure of, the information.

(d) *Exemption if inconsistent with secrecy provisions*

If notification of an eligible date breach would be inconsistent with another legislative act or statutory rule that prohibits or regulates the use or disclosure of information.

(e) *Exemption if serious risk of harm to health and safety*

(i) If the Privacy Officer reasonably believes that notification would create a serious risk of harm to an individual's health or safety. In making this decision the Privacy Officer must:

- consider the extent to which the harm of notifying the breach is greater than the harm of not notifying the breach;
- consider the currency of the information relied on in assessing the serious risk of harm to an individual; and
- not search data held by TAFE NSW, or 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, there is information in the data relevant to whether an exemption under this section applies.

(ii) The Privacy Officer must notify the NSW Privacy Commissioner in writing when TAFE NSW relies on the exemption under this section, including whether the exemption is permanent or temporary (and if temporary, the specified or expected time that the exemption will be relied on).

(f) *Exemption for compromised cyber security*

(i) If the Privacy Officer reasonably believes that notification would worsen TAFE NSW's cyber security or lead to further data breaches.

(ii) The Privacy Officer must notify the NSW Privacy Commissioner in writing when TAFE NSW relies on the exemption under this section for a period of time, including when the exemption is expected to end and of the way in which TAFE NSW will review the exemption. 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.

The exemptions above may not apply where other foreign data protection / privacy legislation applies.

2.7.6 Notifiable Data Breaches Scheme (NDB Scheme) under the Privacy Act 1988 (Cth)

If a data breach involves tax files numbers that TAFE NSW holds or other personal information where TAFE NSW is subject to the *Privacy Act 1988 (Cth),* then TAFE NSW is required under the NDB Scheme to report eligible data breaches (i.e. breaches that are likely to result in serious harm to an individual) to the Office of the Australian Information Commissioner (OAIC) and to affected individuals.

2.7.7 Other legal and contractual obligations to notify

When deciding to notify affected individuals and any other parties about a data breach, TAFE NSW will consider any other legal and contractual obligations that require TAFE NSW to notify them, including any applicable foreign data protection / privacy laws. Some of the other parties TAFE NSW may notify depending on the circumstances, include:

- the Police;
- insurance providers;
- credit card companies and/or financial institutions;
- professional or other regulatory bodies;
- other Government agencies that have a direct relationship with the information; and/or
- any other applicable internal or external parties who have not already been notified.

3. Country-specific data protection laws

3.1 Other country-specific data protection laws, such as the European Union's General Data Protection Regulation (**GDPR**) and China's Personal Information Protection Law (**PIPL**), may also apply to TAFE NSW in certain circumstances, including where TAFE NSW:

- processes personal information of staff, students and alumni who are located in countries covered by the legislation;
- offers goods or services in countries covered by the legislation (e.g. where TAFE NSW promotes courses or training programs to citizens or residents in those countries);

- enters into a contract with an entity located in that country, which involves the processing of personal information and disclosure of it out of that country to TAFE NSW, and vice versa; and
- collaborates with other entities in that country which includes the collecting and processing of personal information.

3.2 While certain provisions of other applicable foreign data protection / privacy laws, including the GDPR and PIPL, will be addressed in this Plan, any requirement to comply with additional provisions will be considered on a case-by-case basis.

4. Complaints

4.1 Making a complaint

4.1.1 If an individual believes that TAFE NSW has breached their privacy, they should contact the responsible business area or unit.

4.1.2 If an individual is not satisfied with the response the response of the responsible business area or unit, they may make a formal complaint about the breach of privacy by contacting the Privacy Officer at privacy@tafensw.edu.au.

4.1.3 An individual may also complain directly to the NSW Privacy Commissioner at:

NSW Privacy Commissioner
Information and Privacy Commission (IPC)
GPO Box 7011, Sydney NSW 2001
Phone: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Website: www.ipc.nsw.gov.au

4.1.4 Individuals that are subject to other country-specific data protection / privacy laws may make a complaint to their relevant privacy authority / commissioner.

4.2 Privacy internal review

4.2.1 Requesting an internal review

(a) If an individual believes TAFE NSW has breached their privacy, they can request an internal review.

(b) An application for internal review must:
- be made in writing to TAFE NSW. You may use the Information and Privacy Commission Internal Review Application Form available at ipc.nsw.gov.au/privacy-compliant-internal-review-application-form;
- include a return address for correspondence;
- be lodged with TAFE NSW within six months of the applicant first becoming aware of the breach that is the subject of the complaint, unless TAFE NSW agrees a later time at its discretion; and
- provide sufficient information for the complaint to be investigated.

(c) As soon as practicable after receiving a valid application for internal review, TAFE NSW must notify the NSW Privacy Commissioner of the application and keep the NSW Privacy Commissioner informed of the progress of the internal review.

4.2.2 Internal review process

(a) An internal review will be conducted by TAFE NSW within 60 days of receiving a valid application, unless an extension is otherwise agreed with the applicant. The Privacy Officer will undertake the internal review on TAFE NSW's behalf unless there is a conflict of interest or the Privacy Officer is unavailable, in which case the internal review will be undertaken an appropriate delegate.

(b) Within 14 days of the completion of the internal review, TAFE NSW will notify the applicant in writing of:

- the findings of the review (and the reasons for those findings);
- any action proposed to be taken by TAFE NSW (and the reasons for taking that action); and
- the right of the applicant to have those findings, and TAFE NSW's proposed action, administratively reviewed by the Tribunal.

(c) TAFE NSW will also inform the Privacy Commissioner of the findings of the internal review and of the action proposed to be taken by TAFE NSW in relation to the matter.

4.2.3 External privacy review

(a) If the applicant is not satisfied with the findings of the internal review, or the action taken by TAFE NSW in relation to the internal review, the applicant may lodge an application for an external review by the Tribunal, at:

NSW Civil and Administrative Tribunal (NCAT)
PO Box K1026
Haymarket NSW 1240
Phone: 1300 006 22

(b) The application must be lodged within 28 days of the applicant receiving notice of an internal review finding. Where an internal review is not completed within 60 days, the 28 day time limit starts when the 60 day period has expired.

Please see the Tribunal website at ncat.nsw.gov.au for more information on the external review process.

5. Education and Training

5.1 Policy and governance

5.1.1 All TAFE NSW staff have privacy obligations and responsibilities under Privacy Laws.

5.1.2 The TAFE NSW Privacy Policy is the primary TAFE NSW instrument governing TAFE NSW's privacy requirements and is supported by this Plan. Privacy requirements are also included in other TAFE NSW policies, procedures and guidelines.

5.1.3 Information, including policies and procedures, about privacy related matters for staff is available on TAFE NSW's intranet. Further advice and guidance on privacy is available upon request from the TAFE NSW Privacy Officer at privacy@tafensw.edu.au.

5.2 Privacy Impact Assessments

When reviewing or implementing projects, processes and information technology systems across TAFE NSW (including third party systems, software and tools) and it may affect an individual's privacy or involve the collection, storage, use or disclosure of personal information, TAFE NSW should undertake a Privacy Impact Assessment.

5.3 Education and training

5.3.1 Privacy requirements and responsibilities are included as part of the TAFE NSW induction and on-boarding program.

5.3.2 TAFE NSW also provides regular education and training to staff to inform them of their obligations and responsibilities under Privacy Laws. Privacy news and updates are also communicated to staff on a regular basis.

5.3.3 Managers and supervisors are responsible for ensuring staff are informed of their privacy responsibilities and undertake appropriate training.

6. Plan updates

This Plan will be reviewed and updated as required to ensure ongoing compliance with all applicable Privacy Laws and to address any changes in legislation, processes, procedures or other events.

APPENDIX 1 - Definitions

Data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Eligible data breach means:

(a) 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

(b) personal information held by TAFE NSW is lost in circumstances where:
  (i) unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and
  (ii) 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 means information or an opinion about:

(a) the physical or mental health or a disability (at any time) of an individual;
(b) an individual's express wishes about the future provision of health services to him or her; or
(c) a health service provided, or to be provided, to an individual.

Health Privacy Principles (HPPs) mean the Health Privacy Principles specified in the HRIA in respect of health information.

Information Privacy Principles (IPPs) mean the Information Privacy Principles specified in the PPIPA in respect of personal information.

Personal information (or otherwise known as personal data) 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 be ascertained from the information or opinion. Unless otherwise specified, Personal information includes health information for the purpose of this Plan.

NSW Privacy Commissioner means the NSW Privacy Commissioner.

Privacy Impact Assessment (PIA) means an assessment of the impacts on privacy of a project, technology, product, service, policy, program or other initiative, and which sets out recommendations for managing, minimising or avoiding that impact.

Privacy Laws mean the *Privacy and Personal Information Protection Act 1998* (NSW) (**PPIP Act**), *Health Records and Information Protection Act 2002* (NSW) (**HRIP Act**), *Privacy Act 1988* (Cth) (where applicable) and any other applicable data protection / privacy laws such as 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.

Public register means a register of personal information that is required by law to be, or is made, publicly available or open to public inspection, whether or not upon payment of a fee.

Staff means any person working in a casual, temporary or permanent capacity at TAFE NSW, including individual consultants and contractors.

TAFE NSW Privacy Policy means TAFE NSW's Privacy Policy which is available at www.tafensw.edu.au/privacy.

Tribunal or **NCAT** means the New South Wales Civil and Administrative Tribunal.