

PC005 Privacy Protection Code of Practice

1. Purpose

This code sets out the expectations on staff in relation to the protection of privacy for all members of the Institute community. It ensures that members of the Institute staff comply with both the Commonwealth Privacy Act (1988) and the Victorian Information Privacy Act (2000).

2. Scope

This Code of Practice refers to all staff of Wodonga TAFE and to any person contracted to carry out work on behalf of the Institute, during the period of that contract.

Breaches of this Code of Practice may result in the initiation of disciplinary action.

3. References

POL07 Privacy Policy
POL15 Staff Conduct Policy
PC001 Staff Code of Conduct
PC002 Financial Propriety Code of Practice
PC003 Conflict of Interest Code of Practice
PC004 Customer Service Code of Practice
PC006 Copyright and Intellectual Property Code of Practice
PC007 Use of Electronic Resources Code of Practice
PP042 Staff Discipline Procedure
PP043 Staff Dispute Conflict Resolution Procedure
PP044 Staff Grievance Procedure
Victorian Information Privacy Act, 2000
Health Records Act, 2001
Commonwealth Privacy Act, 1988
Higher Education Support Act, 2003.

4. Definitions

For the purposes of this code:

Personal information means information about an individual whose identity is clear or can reasonably be worked out from that information. Personal information can include opinions and does not have to be true. Typical personal information includes an individual's name, address, age, financial status and family information. The privacy laws cover information in many forms, including documents, photographs, electronic material (such as voice mail and video recordings) and digital databases.

Sensitive information[†] means information or an opinion about an individual's –

- i) racial or ethnic origin; or
- ii) political opinions; or
- iii) membership of a political association; or
- iv) religious beliefs or affiliations; or
- v) philosophical beliefs; or
- vi) membership of a professional or trade association; or
- vii) membership of a trade union; or
- viii) sexual preferences or practices; or
- ix) criminal record

that is also personal information;

Unique identifier means an identifier (usually a number) assigned by an organisation to an individual uniquely to identify that individual for the purposes of the operations of the organisation but does not include an identifier that consists only of the individual's name.

5. Code

The ten Information Privacy Principles (IPPs) listed below are the practical core of the Victorian Information Privacy Act, 2000. Staff at Wodonga TAFE must be aware of these principles, and fully understand their implications. All business must be conducted accordingly. The principles apply equally to staff, learners or any other members of the Institute community, whether they are individuals, groups or enterprises.

A short summary of each Information Privacy Principle (IPP) is shown in the table below, together with the behavioural expectation incumbent on all staff of the Institute (or those acting on behalf of the Institute) in relation to these principles.

Privacy Principle	Behavioural Expectations
<p>1. Collection</p> <p>Collect only personal information that is lawful and necessary for performance of functions. Advise individuals that they can gain access to personal information</p>	<ul style="list-style-type: none"> a) Before collecting personal information from staff, learners or any other stakeholder groups, ensure that the information collected is necessary for the proper and efficient conduct of Institute business (note the difference between "necessary" and "desirable"). b) As they are developed or reviewed, ensure that forms include a statement on how the information will be used and how individuals can access their personal information if required. c) Ensure that individuals understand the reasons that Wodonga TAFE is collecting and recording personal information. d) Ensure that individuals are aware at the outset, of any external agency who will have access to their personal information. Provide information to individuals about how they can access and review personal information about them held by Wodonga TAFE.

[†] The definition included here is taken directly from Schedule 1 of the Victorian Information Privacy Act, 2000

Privacy Principle	Behavioural Expectations
	<ul style="list-style-type: none"> e) Only collect personal information from the individual themselves, unless the individual has provided (informed) written consent[†]. f) When conducting any human research, ensure that research or survey tools/strategies have been approved by <ul style="list-style-type: none"> i. (internal project) Wodonga TAFE's Human Research and Ethics committee for internal research (as per PP015 Human Research Ethics Procedure), and/or ii. (external project) an external entity's Human Research and Ethics process for research conducted by an external individual or agency.
<p>2. Use and disclosure</p> <p>Use and disclose personal information only for the primary purpose for which it was collected or a secondary purpose the person would reasonably expect. Use for other secondary purposes should have the consent of the person.</p>	<ul style="list-style-type: none"> a) Personal information collected may be used only for the purpose for which it was collected. b) If it is desirable to use the information for an alternative purpose, individuals must first consent in writing. For example. <ul style="list-style-type: none"> i. If you wish to direct market to learners who have already completed a previous course of study, those learners must first consent in writing. ii. If you receive a research request from outside the Institute for data on members of the Institute community where the requested data identifies the individuals concerned, you cannot release the information without the individuals' consent in writing. c) Access Institute data systems only as required as part of your job role (that is, do not use systems such as QLS, TRIM etc to view personal information about staff or learners that does not relate directly to your job role) d) Information collected about individuals may only be disclosed to other parties, with the informed, written consent of the individual. <ul style="list-style-type: none"> i. This includes responding to queries from parents, employers or any other interested parties in relation to learners' attendance, performance or results^{††} ii. It is also prohibited for you to influence processes such as recruitment, selection etc through the

[†] The only exception to this behavioural expectation is where there is a genuine belief that the health and/or safety of an individual is imminently at risk

^{††} When confronted with a request to provide such information, the response here is appropriate: "Unfortunately I am not able to provide you with this information because of current privacy legislation. If you have any further concerns, I can ask my manager to contact you"

Privacy Principle	Behavioural Expectations
	<p>disclosure of personal information about a member of the Institute community, where you are not an official part of that process.</p> <p>iii. Where a member of the Institute community reveals personal information to you, that information may not be shared with other staff or anyone else, even if you believe it to be in the best interests of the individual.</p> <p>e) ensure that learners complete and sign their enrolment forms because that form includes a consent section in relation to release of information as required to OTTE or other government agencies.</p>
<p>3. Data quality</p> <p>Make sure personal information is relevant, accurate, complete and up to date</p>	<p>a) Utilise Institute systems and procedures effectively to ensure that data collected and stored is relevant to the purpose of collection, up to date and complete.</p> <p>b) Provide opportunities for individuals to review personal data stored and confirm its accuracy.</p> <p>c) Provide verified (or verifiable) evidence of accredited training, other professional development and relevant vocational experience to the Institute as required for the purpose of ensuring the currency of information in personnel files.</p>
<p>4. Data security</p> <p>Take reasonable steps to protect personal information from misuse, loss, unauthorised access, modification or disclosure</p>	<p>a) Ensure that paper documents which include information about individual(s) where the individual(s) can be identified are stored securely within department offices or work areas.</p> <p>i. Use lockable TRIM cabinets to store such documents if they are to be retained.</p> <p>ii. Use lockable filing cabinets, or secure, lockable offices to secure documents on a temporary basis.</p> <p>iii. Ensure offices, cupboards or filing cabinets containing such information are in areas that the general Institute population (staff, learners or others) do not have unsupervised access.</p> <p>iv. Lock such cabinets or cupboards when the work area is unattended.</p> <p>b) Dispose of paper documents which include information about individual(s) where the individual(s) can be identified carefully, via Institute shredding bins.</p> <p>c) Protect electronically stored information by</p> <p>i. Ensuring that network access passwords or information system access passwords are not disclosed to any other person.</p> <p>ii. Logging off or locking your computer workstation</p>

Privacy Principle	Behavioural Expectations
	<p>when you move away from your desk.</p> <p>iii. Positioning your workstation so that the screen cannot be viewed by anyone without authorisation to do so.</p> <p>iv. Complying with the expectations as documented in the Institute's PC007 Use of Electronic Equipment Code of Practice.</p>
<p>5. Openness</p> <p>Document clearly expressed policies on management of personal information and provide the policies to anyone who asks</p>	<p>a) Comply with the behavioural expectations as outlined in POL07 Privacy Policy and this document.</p> <p>b) Refer individuals to the Institute's Privacy Policy and provide direction on how to request access to records that contain personal information.</p>
<p>6. Access and correction</p> <p>Individuals have a right to seek access to their personal information and make corrections. Access and correction will be handled by submitting a request in writing to the Institute's Privacy Officer</p>	<p>a) Provide information to members of the Institute population on how to request access to their personal information. Include such information</p> <ul style="list-style-type: none"> i. in handbooks. ii. via website and intranet. iii. On Enrolment forms <p>b) Direct any requests for access to personal information to the Institute's Privacy Officer, i.e. Manager CIAS.</p> <p>c) Take action to correct personal information if individuals inform us it is inaccurate, incomplete or non-current.</p>
<p>7. Unique identifiers[†]</p> <p>A unique identifier is usually a number assigned to an individual in order to identify the person for the purposes of an organisation's operations. Tax File Numbers and Driver's Licence Numbers are examples. Unique identifiers can facilitate data matching. Data matching can diminish privacy. IPP 7 limits the adoption and sharing of unique identifiers</p>	<p>a) Assign unique identifiers to learners (via QLS) and to staff (according to the staff numbering convention) for the purpose of effectively managing records and files.</p> <p>b) If individuals' unique identifiers for other organisations are provided to us for any reason, this information is not to be retained unless it is required for the operation of the Institute. For example</p> <ul style="list-style-type: none"> i. A learner may provide a driver's license as proof of identity when presenting for an assessment activity. ii. A learner may provide a health care card as evidence to support their claim for a fee concession. iii. A staff member may provide originals of qualifications or statements of attainment gained from other educational providers. iv. A staff member may provide a medical certificate in

[†] see definition on page 2 of this code of practice

Privacy Principle	Behavioural Expectations
	<p>support of a sick leave claim, which displays their Medicare Number.</p> <p>c) In these examples, photocopies of such evidence may be retained but, after copying, the unique identifiers should be blocked out.</p> <p>d) If the use, or disclosure to another entity, of such identifiers is required as part of Institute operation, then signed consent must be obtained from the individual before it is used or disclosed.</p> <p>e) A unique TRIM file will be established for each student that will contain information related to students such as enrolment forms, qualifications, achievements, correspondence, and fee payment arrangements.</p> <p>f) Access to individual TRIM files will be determined by the Department Manager and administered by the Team Leader – Records.</p>
<p>8. Anonymity</p> <p>Give individuals the option of not identifying themselves when entering transactions with organisations, if that would be lawful and feasible.</p>	<p>a) Allow members of the Institute population to remain anonymous when providing feedback on the quality of Institute services and / or program delivery and assessment.</p> <p>b) Where members of the Institute community elect to remain anonymous in other Institute processes, they must be informed about the likely consequences of that choice.</p>
<p>9. Transborder data flows</p> <p>Basically, if your personal information travels, your privacy protection should travel with it. Transfer of personal information outside Victoria is restricted. Personal information may be transferred only if the recipient protects privacy under standards similar to Victoria's IPPs.</p>	<p>a) Personal information about members of the Institute community must not be disclosed to individuals or entities outside Victoria unless</p> <ul style="list-style-type: none"> i. The individual provides a written request or written consent. ii. The information is required by a federal or state agency with whom Wodonga TAFE has a contractual agreement.
<p>10. Sensitive information^{††}</p> <p>The law restricts collection of sensitive information like an individual's racial or ethnic origin, political views, religious beliefs, sexual preferences, membership of groups or criminal record.</p>	<p>a) Information about ethnic origin of learners may be collected on enrolment for the purpose of providing statistical information to government agencies and accessing government support.</p> <p>b) Information about the language, literacy and numeracy standards of individual learners may be collected on enrolment, or during an enrolment period, for the purpose of providing appropriate learning and assessment support.</p>

^{††}See definition on page 1 of this Code of Practice

Privacy Principle	Behavioural Expectations
	<p>c) Information about criminal records for staff or prospective employees may be requested in accordance with the regulations as specified by</p> <ul style="list-style-type: none"> i. Victoria Police ii. NSW Department of Education and Training Working with Children Screening Branch. <p>Information returned after such checks must not be retained by the Institute (however, evidence that the check has been performed must be retained).</p> <p>d) Do not seek or request the provision of other sensitive information about any members of the Institute community.</p> <p>e) If any such sensitive information is provided to you voluntarily by a member of the Institute community</p> <ul style="list-style-type: none"> i. You may not disclose that information to any other person and ii. You may not document or retain any record of that information without the written consent of the individual concerned or unless you genuinely believe that the disclosure of such information will protect someone's health or safety. iii. You must not allow the knowledge you gain through such a disclosure of sensitive information to influence you in any way that is detrimental to the individual concerned.