Privacy of Student Personal Information Policy

Navitas Professional Institute

Document

Document I.D.	NPI 23 [22] 15P Privacy of Student Personal Information Policy		
Policy Owner	Registrar		
Initial Issue Date	21 November 2012		
Endorsed by	Executive Committee	**Date Endorsed**	21 November 2012
Approved by	Principal & Executive General Manager	**Date Approved**	17 July 2013
Initial Approver	Executive Committee	**Date Initial Approval**	21 November 2012

Version Control

Issue Date:	Summary of Changes	Review Date
21 November 2012	Policy established (Replaced Personal Information Policy)	November 2017
17 July 2013	Administrative review and amendment	July 2017
01 September 2015	Administrative update to new template and update related laws and regulations	July 2017
25 January 2016	Minor template technical amendments	July 2017

Privacy of Student Personal Information Policy

1. Purpose and Scope

The college is committed to protecting the privacy of students' personal information.

The purpose of this policy is to regulate the collection, management, use and disclosure of personal information by the college to maintain and protect the privacy of students information in accordance with the Privacy Act 1988 (Cth).

This policy reflects the college's commitment to building a culture of integrity, equity and social justice as an integral part of its mission.

This policy applies to all student personal information collected and held by the college, its staff and those contracted to provide services to and on behalf of the college.

2. Policy

2.1 Statement of Commitment

The college is committed to maintaining and respecting the privacy of all students and prospective students of the college. This policy and the practices that the college follows conform to the Privacy Act 1988 (Cth), the Privacy Amendment Act 2000 (Cth) and the National Privacy Principles (NPP).

The college is committed to protecting the privacy of student personal information and this commitment is reinforced by legislation.

The college recognises the importance for students to be confident in knowing their personal information is protected and is used only for the purpose for which it was collected.

The college undertakes to ensure:

- That release of information is consistent with applicable Australian laws, regulations and guidelines, as amended from time to time, and
- That all reasonable steps are taken by the college to protect student personal information

2.2 Collection

The college will only collect information about a student where this is necessary for one or more of its functions or activities.

When the college collects information about a student, it will take reasonable steps to inform the student of:

- the purposes for which the information is collected;
- to whom we would usually disclose this kind of information (if applicable);
- any law that requires the particular information to be collected; and
- the main consequences (if any) for the student if he or she does not provide all or part of the information.

Some personal information, such as information about a student's ethnicity or sensitive or health information will only be collected with the consent of the student concerned, or as otherwise allowed by law or required or authorised by law.

The student's personal information will normally be collected from the student concerned, however, there may be occasions when information is transferred from third parties, such as a family member who contacts the college on the individual's behalf; from the college contractors who supply services to the college; through partner institutions or from a publicly maintained record. When this occurs, the college staff concerned will either be satisfied that the student is aware of the transfer of information or will take reasonable steps to ensure that the student is aware that this has occurred.

If a student does not provide information requested by the college, it may not be able to provide services to the student.

2.3 Use and Disclosure

To the extent required by the Privacy Act 1988 (Cth), the college will only use or disclose students' personal information:

- for the purpose for which it was collected (the primary purpose);
- for a secondary purpose that:

    1. is related to the primary purpose (if the information is sensitive information or health information, it will only be used or disclosed for a secondary purpose which is directly related to the primary purpose); and
    2. the student would reasonably expect his or her information to be used or disclosed for this secondary purpose; or
    3. where there is consent of the student concerned to the use or disclosure; or
    4. as otherwise allowed under the Act, or required or authorised by or under law.

When the college collects information from a student, the purposes for which the information is collected will usually be made clear on any forms that are to be completed, or will otherwise be apparent from the circumstances.

If the college is required to use or disclose student information for purposes other than the primary purpose or the reasonably expected secondary purpose, it will endeavour to seek the student's consent prior to such use or disclosure unless for reasons otherwise stated in this policy.

Students should be aware that personal information will be used by staff involved in the administration of an application, enrolment, academic progression, placement, graduation and the provision of student services. The names of students will appear on class lists and online class spaces as part of the normal learning and teaching practices of the college. The names of graduates and their awards are published in the college graduation booklet for each ceremony and may appear on the college website.

Staff may use student personal information for directly related purposes in ways that a person would reasonably expect, such as to contact students to participate in satisfaction surveys that help the college evaluate and improve services.

The college may also share student personal information with third party providers, such as market research firms or electronic storage providers, who are engaged to provide certain services to the college. Where student personal information is disclosed to third parties, the college will not allow the use of that information for any purpose other than the purpose for which it was disclosed.

The college will advise students at the time of data collection that from time to time, the college may share student personal information, for example contact details, within the Navitas Group and that information will be used to offer or notify students of products, services or other information that Navitas reasonably believes may interest them.

If students require more specific information about the way in which their information is used or disclosed, they are advised to contact the relevant college area collecting the information or alternatively, to contact the Registrar.

Students have the right to decline to have their personal information shared, or to receive marketing or other offers from the Navitas Group. This option will be available at time of data collection, and thereafter, the student may withdraw at any time by advising the college by phone on 1800 061 199 or info@acpc.edu.au.

2.3.1 Release of Information if there are serious threats to life, health or safety

National Privacy Principle NPP 2.1(e) makes provision for an organisation to release personal and/or sensitive information where it reasonably believes that the use or disclosure is necessary to lessen or prevent:

(i) a serious and imminent threat to an individual's life, health or safety; or
(ii) a serious threat to public health or public safety.

This exception is aimed at emergency situations where there is a serious threat to health and safety and using or disclosing personal information will help reduce that threat.

Ordinarily a serious threat would be a threat of bodily injury, threat to mental health, illness or death. 'Imminent' means the threatened harm is about to happen.

If a staff member forms a belief that there is an imminent threat then the Principal and Executive General Manager must be immediately informed. The Principal and Executive General Manager has the authority to act on the college's behalf and release information under NPP 2.1 (e).

2.3.2 Lawful disclosure of information

The college may disclose information in accordance with the Privacy Act 1988 (Cth).The college may be required to disclose some student personal information to State or Commonwealth government agencies to comply with other laws, for example to report tax file numbers, provide statistics, meet mandatory reporting requirements to departments such as Centrelink and DIAC.

The college may disclose personal information in exceptional circumstances if it is considered imperative for reasons of health and safety. The college may also be required to provide students' personal information as evidence in court or tribunals, to police services or other law enforcement agencies under subpoena, police search warrant or other similar written official request. In these cases the Principal and Executive General Manager must approve the disclosure of information.

Copies of an individual's testamur, statement of results or statement of attainment may also be provided by the college under specific legislation including the Higher Education Support Act 2003 and Education Services for Overseas Students Act 2000

2.4 Data Quality

The college will take reasonable steps to ensure that the information it holds about students is accurate, complete and up-to-date.

2.5 Data Security

The college will take reasonable steps to protect information from misuse, loss, unauthorised access, modification or unauthorised disclosure.

The college will take reasonable steps to destroy or permanently de-identify any information that is no longer needed for any purpose in accordance with the Records Management Policy.

2.6 Openness

If requested, the college will take reasonable steps to inform the student making the request of what personal information it holds and how it collects, holds, uses and discloses that information.

2.7 Access & Correction

Access to and correction of student personal information is handled by the college in accordance with the provisions of the Privacy Act 1988 (Cth) and the Freedom of Information Act 1982 (Cth).

The College will provide access to personal information held about the student on request by that student.

Students are able to view and update much of their personal and enrolment information through the online student portal.

If a student wishes to view personal information that is not accessible through the online student portal, then the college requires such a request to be in writing to the Registrar's office. The student must provide proof of identity with the application for access.

If a student is able to establish that information held by the college is inaccurate, out-of-date or incomplete, he or she may request the college to correct the personal information. The college will correct any incorrect personal information upon production of documentation verifying the change and will not refuse to make a correction without giving reasons.

If the college refuses to make a correction due to disagreement with the student over whether the information is inaccurate, out-of-date or incomplete, it will take reasonable steps to place a statement

from the student associated with the information that in the student's opinion the information is inaccurate, out-of-date or incomplete.

There is no charge for lodging a request for access to student personal information but the college may charge for the time involved in providing this access and for associated costs such as photocopying; however, these charges will not be excessive.

2.7.1 Declining Access to Personal Information

National Privacy Principle NPP 6.1(b) allows for an organisation to deny a student access to their personal information in special circumstances, such as, but not limited to:

- in the case of *personal information* other than health information, providing access would pose a serious and imminent threat to the life or health of any individual; or
- in the case of *health information*, providing access would pose a serious threat to the life or health of any individual; or
- providing access would have an unreasonable impact upon the privacy of other individuals; or
- the information relates to existing or anticipated legal proceedings; or
- providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
- providing access would be unlawful; or
- denying access is required or authorised by or under law; or
- providing access would be likely to prejudice an investigation of possible unlawful activity; or
- an enforcement body performing a lawful security function asks the organisation not to provide access to the information.

2.8 Unique Identifiers

The college will not assign a college unique identifier to a student unless it is necessary to carry out the college's functions efficiently (for example, student ID numbers). the college will not adopt a unique identifier assigned to a student by another organisation (for example, Driver's Licence number) unless it is necessary to carry out the college's functions efficiently or the college has obtained the student's consent.

2.8.1 Australian Government-Unique Student Identifier (USI)

The college will record your USI number to enable linking your national vocational training to the National Vocational Education and Training (VET) Data Collection, allowing you to see all of your training results from all providers including all completed training units and qualifications completed with the college. Your application to enrol in a course at the college implies consent for the college to use personal information provided by you during the enrolment process to:

- Generate a USI on your behalf; or
- Validate your USI after you have provided it to the college

2.9 Anonymity

The college will provide students with the option of remaining anonymous in their dealings with the college where this is lawful and practicable.

2.10 Transborder Data Flows

The college may retain other companies and contractors to provide services, including entities located outside Australia, who will need to have access to student personal information to perform their obligations. The college may also use a cloud-based service to store and process personal information. By providing the college with personal information, the student consents to the college disclosing that information to entities located outside Australia for these purposes, on the basis that the college will take reasonable steps to ensure that any overseas recipient complies with NPP or substantially similar principles. Exceptions are found in the NPP section 9, for example when all of the following apply:

- The transfer is of benefit to the student;
- It is impracticable to obtain the consent of the student to the transfer;
- If it were practicable to obtain such consent, the individual would be likely to give it.

2.11 Sensitive Information

The college will not collect sensitive information about an student unless-

- the student has consented; or
- the collection is required by law; or
- the collection is necessary to prevent or lessen a serious threat to the life or health of any student.

Although all personal information should be considered sensitive, an individual may indicate that some of his or her information is particularly sensitive. Examples of highly sensitive information include ethnicity, sexual preference, Tax file numbers, criminal record checks and medical/health conditions.

If it is necessary for sensitive information to be given to a college staff member in connection with the provision of a service or business function, then the college will take steps to prevent unauthorised use or disclosure of the information. the college will adhere to all legislative requirements in relation to the secure storage and/or transmission of sensitive information.

2.11.1 Health Information

In so far as the college holds any health information, it will comply with the Health Privacy Principles set out in the Health Records and Information Protection Acts in the states in which it operates.

2.11.2 Use of Health Information in training

Each state has a Health Records and Information Privacy or Protection Act which regulates the collection, handling and storage of health information by public and private sector health service providers.

Health information is a specific type of personal information. It includes information or an opinion about the physical or mental health or a disability of an individual.

In the provision of education & training, employees and students of the college may use health information, for example in the supervision of clinical practice. Employees of the college will use de-identified information. The college will ensure the consent is informed and freely given.

Classroom discussions and assessments may elicit the disclosure by a student of his or her personal information. The college will inform students at admission that personal information may be the subject of unit assignments or in a class discussion. Under the Health Information Acts, this would generally be considered a directly related secondary purpose within the reasonable expectations of the person. The college is committed to protecting the privacy of student personal information by putting in place processes to mitigate the misuse or unauthorised disclosure of a student's personal information.

2.12 Complaints

If a student believes their privacy has been interfered with, in the first instance they should complain using the Non Academic Grievances and Appeals Policy and Procedure.

If a student is dissatisfied with the outcome of the college process, the student can make a complaint to the Office of the Australian Privacy Commissioner.

3. Responsibilities

The executive and management staff are responsible for assisting in ensuring the effectiveness of the implementation of this policy. This includes ensuring the college employees in their supervision are aware of this policy and their responsibilities as defined herein.

The college employees are responsible for being aware of and complying with this policy.

The Principal and Executive General Manager is ultimately responsible for ensuring the privacy of student personal information held by the college is protected.

Relevant functional managers are responsible for:

- Implementing secure storage procedures for personal information
- Taking reasonable steps to ensure information collected is accurate, complete and current
- Ensuring they have systems for secure transfer, storage and destruction of physical and digital records of personal information.

4. Definitions

Unless the contrary intention is expressed in this policy, the following words (when used in this policy) have the meaning set out below provided by the Office of the Federal Privacy Commissioner:

Academic staff/teaching staff refers to permanent and casual employees engaged in teaching and assessment of courses at the institution.

Access involves giving student information held by the organisation to the student whose information it is. Giving access may include allowing a student to inspect personal information held about them or giving a copy of that information to them.

Collection is the gathering, acquisition or obtaining of personal information from any source and by any means. Collection includes when an organisation keeps personal information it has come across by accident or has not asked for.

"Commonwealth" (Cth) refers to Commonwealth government agencies such as DEEWR (Department of Education, Employment and Workplace Relations), ATO (Australian Taxation Office), Centrelink, DIAC (Department of Immigration and Citizenship)

Consent means voluntary agreement to some act, practice or purpose. It has two elements: knowledge of the matter agreed to, and voluntary agreement. Consent can be express or implied. Express consent is given explicitly, either orally or in writing. Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the student and the organisation

Disclosure: in general terms an organisation discloses personal information when it releases information to others outside the organisation. It does not include giving students information about themselves (this is 'access', see above)

Health information is a particular kind of 'personal information' and attracts additional privacy protection because of its greater sensitivity. 'Health information' includes information about a person's health, disability, use of health services, or other personal information collected from someone when delivering a health service.

Institution (the)/College (the) means the Navitas Professional Institute and its colleges (see registration information below).

International student/ Overseas student means a student required to hold a student visa for study in Australia.

National Privacy Principles (NPP) refers to Schedule 3 of the Privacy Act 1988 (Cth).

Personal Information is defined as "information or an opinion (including information or an opinion forming part of a database) whether true or not, and whether recorded in material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion." (Privacy Act 1988, Section 6.)

It includes all personal information regardless of its source.

Privacy refers to the type of privacy covered by the Privacy Act and this policy and refers to the protection of people's personal information.

Sensitive information is a subset of personal information. It means information or opinion about a student's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record or health information about a student (Privacy Act 1988, Section 6.)

Tax File Number is defined by the TFN Guidelines as generally meaning a unique number issued to the person by the Commissioner of Taxation under certain provisions of taxation law to identify

students, companies and others who lodge income tax returns with the Australian Taxation Office (ATO). The TFN Guidelines protect the TFN information of students only. The obligations on an organisation relating to the collection of TFNs under the TFN Guidelines are in addition to responsibilities under the National Privacy Principles, Information Privacy Principles and other legislation e.g. taxation laws, superannuation laws, personal assistance laws, secrecy laws and the Data-matching Program (Assistance and Tax) Act 1990 (Cth).

Unit means a unit of study in a higher education course or a unit of study, subject, module and/or unit of competency in a vocational education and training course.

Use refers to, in general terms, use of personal information and includes the handling of personal information within an organisation including 'the inclusion of information in a publication'.

5. Review

This policy is reviewed at a minimum of every 5 years by the policy owner (or designate) to ensure alignment to appropriate strategic direction and its continued relevance to Navitas' current and planned operations.

The next scheduled review of this document is listed in the Version Control section on Page 1.

6. Records

Records in association with this policy will be kept in accordance with the institution's Records Management Policy and Records Retention and Disposal Schedule. Confidential files related to the implementation of the policy must be maintained according to relevant privacy processes.

7. Related documents

College website Privacy Statement; College website Unique Student Identifier Privacy Notice; Record Management Policy and Records Retention and Disposal Schedule; Procedures for Privacy of Student Information v2; Student Information Sheet: How to access and correct personal information held by the college; Non-Academic Grievances, Complaints and Appeals Policy and Procedure and NVT Privacy http://navitas.com/privacy_policy.html.

8. Related legislation

Privacy Act 1988(Cth); Privacy Amendment (Private Sector) Act 2000 (Cth); Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth); Relevant states and territories privacy acts; Relevant states and territories Health Records and Information Privacy or Protection ; Data-matching Program (Assistance and Tax) Act 1990 (Cth); Tax File Number Guidelines 2011 (TFN Guidelines) issued under s 17 of the Privacy Act 1988 (Privacy Act); Freedom of Information Act 1982 (Cth); Higher Education Support Act 2003 (HESA) (CTth); Education Services for Overseas Students (ESOS) Act 2000; National Vocational Education and Training Regulator Act 2011 (Cth), Data Provision Requirements 2012 and Student Identifiers Act 2014 (Cth).

Registration information

The Navitas Professional Institute is a group of colleges in the Navitas Professional and English Programs (PEP) Division of Navitas Limited the colleges being the Australian College of Applied Psychology (ACAP), Navitas College of Public Safety (NCPS), Health Skills Australia (HSA), and the Australian TESOL Training Centre (ATTC) with respect to ATTC's 39296QLD Graduate Certificate in TESOL and 39297QLD Graduate Diploma in TESOL courses. Navitas Professional Institute Pty Ltd (NPI Pty Ltd), ABN 94 057 495 299, National CRICOS Provider Code 01328A, TEQSA HE Provider Registration Code 12009, RTO 0500. Health Skills Australia Pty Ltd ABN 53 123 479 201, RTO 21646.