



**Education &  
Communities**

# **PRIVACY MANAGEMENT PLAN FOR DEPARTMENT OF EDUCATION AND COMMUNITIES**

MARCH 2014



# TABLE OF CONTENTS

## **Part 1 Introduction**

1. Introduction
2. Terms and their meanings
3. The Department's functions and activities

## **Part 2 Personal and Health Information**

4. Personal information
5. Health information
6. Public Registers
7. Personal and Health information held by the Department
8. Information Protection Principles (IPPs)
9. Health Privacy Principles (HPPs)

## **Part 3 Application of Information Protection Principles and Health Privacy Principles**

10. Collection of personal and health information
11. Retention and Security of personal and health information
12. Access to personal and health information
13. Alteration of personal and health information
14. Accuracy of personal and health information
15. Use of personal Information
16. Disclosure of personal information
17. Special Restrictions on Disclosure of personal information
18. Use and disclosure of health information
19. Identifiers
20. Anonymity and health information
21. Transborder data flows and data flow to the Commonwealth of health information
22. Linkage of health information
23. Compliance with identifiers anonymity, transborder data flow and linkage principles

## **Part 4 Internal Review**

24. Complaints – Internal Review Procedures

## **Part 5 Implementation of Privacy Management Plan**

25. Legislation affecting the Department's processing of information
26. Policies affecting the Department's processing of information
27. Dissemination of Policies and Training
28. Responsibilities
29. Contractual Arrangements

## **Part 6 Annexures**

30. [Annexure 1](#) – Application for access to the applicant’s personal and or health information made in accordance with the *Privacy and Personal Information Protection Act 1998* and/or *Health Records and Information Privacy Act 2002*
  
31. [Annexure 2](#) – Application for alteration of the applicant’s personal and or health information made in accordance with the *Privacy and Personal Information Protection Act 1998* and/or *Health Records and Information Privacy Act 2002*

## PART 1

### 1. Introduction

#### 1.1 Legislative framework

The [Privacy and Personal Information Protection Act 1998](#) (PPIPA) requires public sector agencies to prepare and implement a Privacy Management Plan detailing the policies and practices which ensure the agency's compliance with requirements of both the PPIPA and the [Health Records and Information Privacy Act 2002](#) (HRIPA).

#### 1.2 Object

The object of this Privacy Management Plan (the plan) is to inform:

- Members of the community of how the Department of Education and Communities (the Department) manages and protects their personal and health information, the procedures for requesting access to and alteration of this information and how to request an internal review if aggrieved by the way in which the Department has handled their information, and
- Department staff members of their obligations in relation to handling personal and health information and the relevant policies, procedures and other resources they can access to guide and inform them in meeting the requirements of privacy legislation.

#### 1.3 Amendment

This plan replaces all previous privacy management plans. It will be updated and reviewed biennially to include changes in legislation and administrative or systemic procedures which impact on the management of personal or health information held by the Department.

#### 1.4 Application

This plan applies to all Department staff and covers statutory authorities, agencies and divisions within the four portfolios of the Department with the exception of the Sydney Olympic Park Authority, Venues NSW and The ANZAC Memorial Building Trust.

### 2. Terms and their Meanings

Word/Term	Meaning
authorised representative	Defined in the HRIPA as: an attorney for an individual under an enduring power of attorney, a guardian or person responsible within the meaning of the <a href="#">Guardianship Act 1987</a> , a person with parental responsibility for a child or a person who is legally authorised to exercise functions as an agent of or in the best interests of the individual.
health information	See 5.2
health service	includes a number of services provided as a public or private service and includes psychology services. A full list of the services is at section 4 of the HRIPA.

health service provider	an organisation that provides a health service but does not include an organisation that arranges for health services to be provided to an individual by another organisation.
held	Personal information is held by the Department if it is in possession or control of the information or the information is in the possession or control of a person employed or engaged by the Department in the course of their employment or engagement or the information is contained in a State record in response of which the agency is responsible under the <i>State Records Act 1998</i> .
identifier	an identifier (usually a number) but not an identifier that consists of only an individual's name, that is assigned to an individual in conjunction with or in relation to the individual's health information by an organisation for the purpose of uniquely identifying that individual, whether or not it is subsequently used otherwise than in conjunction with or in relation to health information or is adopted, used or disclosed in conjunction with or in relation to the individual's health information by an organisation for the purpose of uniquely identifying that individual.
investigative agency	Means any of the following: Ombudsman's Office, Independent Commission Against Corruption, Inspector of the Independent Commission Against Corruption, Police Integrity Commission, Inspector of the Police Integrity Commission and any staff of the Inspector, Health Care Complaints Commission, Office of Legal Services Commissioner, a person or body prescribed by the regulations.
law enforcement agency	NSW Police Force, or the police force of another State or a Territory, NSW Crime Commission, Australian Federal Police, Australian Crime Commission, Director of Public Prosecutions of NSW, another State or a Territory, or of the Commonwealth, Department of Corrective Services, Department of Juvenile Justice, Office of the Sheriff of New South Wales or a person or body prescribed by the regulations.
personal information	See 4.2
public register	See 6
staff	an employee or person engaged by the Department

### 3. The Department's Functions and Activities

In 2011, the NSW Government brought Children's Services and parts of Communities NSW, Aboriginal Affairs and the Office of Veterans Affairs (including the ANZAC Memorial Building) together with the Department of Education and Training to create the [Department of Education and Communities](#). The Department is grouped into the following portfolios:

#### 3.1 [Public Schools NSW](#)

Provides advice and guidance to principals in NSW government schools which number over 2,240 and implements strategies to improve the educational and learning outcomes for all students. In line with aims of the National Partnership Agreement on Empowering Local Schools, the portfolio introduced a new model of support to schools in 2013. There are now 4 Executive Directors and 65 Directors of Public Schools who provide support to principals grouped into 65 school networks.

### 3.2 [NSW Technical and Further Education Commission](#) (TAFE NSW)

Operates through its various State offices and 10 individual Institutes:- Hunter, Illawarra, New England, North Coast, Northern Sydney, Riverina, South Western Sydney, Sydney, Western and Western Sydney with a total of 130 campuses across NSW. TAFE NSW manages more than 500,000 enrolments each year and offers over 1,200 nationally recognised vocational qualifications.

### 3.3 [Office of Education](#)

Provides strategic analysis and advice on cross-sectorial, state-wide and national developments across the full spectrum of education and training. The office is responsible for Commonwealth and State issues including National Partnerships, non-government schooling policy, the funding and regulation of providers of early childhood education and care and management of the vocational education and training market in NSW. It has a planning role which encompasses corporate planning and reporting and whole-of-government co-ordination under NSW 2012 (State Plan).

### 3.4 [Office of Communities](#)

Provides a range of government services that share a common focus on strong inclusive and active communities through:

- fostering opportunities and partnerships with community groups,
- overseeing and driving the implementation of the NSW Government Plan for Aboriginal affairs, OCHRE (Opportunity, Choice, Healing, Responsibility, Empowerment),
- arranging and supporting participatory activities such as sport, recreation, local community events, volunteering and veterans' commemorative activities,
- providing community infrastructure that encourages participation such as major sporting precincts, the Sydney Olympic Park, Penrith Lakes and the ANZAC Memorial Building,
- engaging communities and forging coalitions to help them build on their strengths and develop economically, socially and culturally,
- providing opportunities for children and young people to participate in their communities and in decisions that affect them.

## **PART 2**

### **4. Personal Information**

4.1 The PPIPA provides for the protection of personal information held by government agencies.

4.2 What is personal information?

Personal Information is information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about a person whose identity is apparent or can reasonably be ascertained from the

information or opinion. It is not restricted to information that clearly identifies a person but may include information which leads to the identification of an individual when considered in association with other available information. It covers information held in paper or electronic records and extends to images, body samples and biometric data such as fingerprints.

#### 4.3 What information is not personal information?

There are a number of exceptions to the definition of personal information. Those most relevant to information held by the Department are information about:

- an individual who has been dead for more than 30 years,
- an individual that is contained in a publicly available publication,
- an individual that is contained in a public interest disclosure or that has been collected in the course of investigation arising out of a public interest disclosure,
- an individual's suitability for appointment or employment as a public sector official.

## 5. Health Information

5.1 The HRIPA regulates the collection and handling of health information by public sector agencies and private organisations.

#### 5.2 What is health information?

Health information is personal information that is information or an opinion about an individual's physical or mental disability or the provision of a health service to an individual. It includes information about an individual collected in connection with the donation of body parts and genetic information about an individual.

#### 5.3 What information is not health information?

The HRIPA defines personal information in similar terms as the PPIPA with the same exceptions as that Act. Health information, therefore, does not include information about:

- an individual who has been dead for more than 30 years,
- an individual that is contained in a publicly available publication,
- an individual that is contained in a public interest disclosure or that has been collected in the course of investigation arising out of a public interest disclosure,
- an individual's suitability for appointment or employment as a public sector official.

## 6. Public registers

6.1 A public register is defined by the PPIPA as a register containing personal information that is made publicly available or open to public inspection. Health information is included as personal information on public registers.

6.2 Some registers are exempted from the requirements in the PPIPA relating to public registers because the information contained in the register falls within one of the exceptions to the definition of "personal information".

- 6.3 A register which has, and is authorised to have, its entire contents published in a publicly available publication would not be a public register within the meaning of the PPIPA. In addition, if access to a register is given only to specific categories of people rather than to the public at large, then it may not be a public register within the meaning of the PPIPA because it is not “publicly available or open to public inspection”.
- 6.4 The Department is required to record in the [register of government contracts](#) all contracts it enters into with the private sector which are valued at over \$150,000. This is published in the Department of Education and Communities’ section of the [NSW eTendering website](#).
- 6.5 Business units that administer a public register will need to analyse the public register provisions of the PPIPA and, to the extent to which they apply to those registers, will adopt strategies for compliance with PPIPA’s requirements. In summary, those requirements are that:
- before disclosing any personal information from a public register, the Department must be sure that the information is to be used for a purpose relating to the purpose of the register or of the legislation under which the register is kept,
  - the Department may require any person who applies to inspect personal information in a public register to give particulars in the form of a statutory declaration as to the intended use of the information obtained from the inspection,
  - where the Department suppresses, on request, a person’s information from a public register the Department must be satisfied that the safety or well-being of the person will be adversely affected by not suppressing the information and that the suppression is not against the public interest.
- 6.6 Registers which do not fall within the public register requirements of the PPIPA such as the [Pecuniary and Private Interest Register](#) and the [Register of Gifts and Benefits](#) are still subject to the privacy information principles in the PPIPA.

## 7. Personal and health information held by the Department (information)

The Department collects and handles a significant volume of information in the administration and provision of quality education, training and community services.

The main classes of information held by the Department are:

- 7.1 Employee information including:
- personal details such as address, phone number, emergency contact details, tax file number and bank details;
  - records of race, sex, marital status and impairment of employees for equal employment opportunity purposes;
  - medical assessments, certificates and reports;
  - attendance, pay and leave records;
  - recruitment, promotion, appeals and transfer records including the outcome of criminal record checks and working with children checks;
  - service and administrative records;
  - stored electronic messages;
  - performance and disciplinary records;
  - training, apprenticeship and study records; and
  - occupational health and safety and workers compensation records.



## 7.2 Student information including:

- family information including parent/carer occupation and education, address and phone number; languages spoken in the home and emergency details, family court orders, apprehended violence orders,
- student details such as age, gender, residency status, ethnicity, first language, religion, Aboriginality, previous schooling and care arrangements,
- medical information including details of disability, special needs, health care procedures, medication and counsellor records,
- support services accessed by students including services from outside agencies,
- information about children and young person's safety, welfare or wellbeing recorded in reports to Community Services and the Child Wellbeing Unit and information obtained under Chapter [16A Children and Young Person's Care and Protection Act 1998](#),
- discipline and behaviour records including records of violent behaviour,
- accident/incident records and witness statements prepared by students,
- academic results and other achievements including awards and assessments,
- financial information such as Centrelink benefits and credit card details,
- tax file numbers of students when required for purposes such as accessing Vocational Education and Training fee help and fee help loans.

## 7.3 Other stakeholder information including:

- contact details of individuals including email and postal addresses and e-banking details,
- court orders,
- information about individuals and organisations obtained during the tender process,
- information about individuals and organisations obtained in the course of developing and managing business relationships and maintaining contractual relationships,
- information obtained in the course of complaint handling including confidential information exchanged at mediation.

## 8. Information Protection Principles (IPPs)

### 8.1 The PPIPA applies [12 IPPs](#) to the way in which personal information is handled. The IPPs regulate the:

- collection,
- storage,
- access,
- alteration,
- accuracy
- use and
- disclosure

of personal information. They can be found at [sections 8 to 19](#) of the [PPIPA](#). These are dealt with in more detail at points 10-18.

### 8.2 Exceptions to the IPPs

There are a number of exceptions to the IPPs, for instance a public sector agency does not have to comply with some IPPs when non-compliance is authorised or permitted under another Act. The exceptions are dealt with in more detail at points 10 – 18.

### 8.3 Modification of the IPPs

The PPIPA allows for the operation of privacy codes of practice that may modify the application of IPPs to a public sector agency. The privacy codes of practice that impact on the operation of the Department are:

- The Department of Education and Training [Privacy Code of Practice](#) which modifies the application IPPs as they relate to the Department's functions in the areas of child protection, parental/caregiver involvement, complaint handling and investigative procedures and maintaining a secure and disciplined working environment. The modifications are dealt with in more detail at points 10 - 18.
- The [Privacy Code of Practice \(General\) 2003](#) which applies to agencies that provide education, welfare, health, mental health, disability, drug and alcohol, housing and support services. It modifies the application of the collection, use and disclosure IPPs when authorised by a senior officer of an agency. In most instances these modifications are covered by [Chapter 16 of the Children and Young Peoples \(Care and Protection\) Act 1998](#) which allows for the exchange of information between agencies that have responsibilities relating to the safety, welfare or well-being of children and young persons.

### 8.4 The PPIPA allows the Privacy Commissioner to make [Public Interest Directions](#) to waive or modify the requirement of a public sector agency to comply with an IPP. The current directions which impact on the functions of the Department are:

- *Direction relating to the collection of Personal Information About Third Parties by NSW Public sector (Human Service) Agencies from their Clients:-* modifies collection IPPs.
- *Direction relating to the Redfern Waterloo Case Coordination Project:-* modifies collection, use and disclosure IPPs
- *Direction relating to the Disclosure of Information by the NSW Public Sector Agencies for Research Purposes:-* modifies disclosure IPPs for research purposes.
- *Direction on disclosures of information by NSW Public Sector Agencies to the National Coronial Information System (NCIS):-* modifies the disclosure IPP to allow for disclosure of information for inclusion in the NCIS.
- *Direction on the disclosures of information to victims of crime:-* modifies the collection, use and disclosure IPPs.
- *Direction for the Department of Family and Community Services and Associated Agencies:-* applies to Aboriginal Affairs and modifies the collection, use and disclosure IPPs to allow for involvement of guardians or next most appropriate person where an individual does not have capacity to make decisions under the Privacy Act.
- *Direction on the Processing of Personal Information by NSW Public Sector Agencies in relation to their Investigative Functions:-* modifies the collection, use and disclosure IPPs in the exercise of an agency's investigative functions.
- *Direction on Information Transfers between NSW Public Sector Agencies:-* modifies the disclosure of information to other government agencies in particular circumstances.

## 9. Health Privacy Principles (HPPs)

9.1 The HRIPA applies 15 HPPs to the handling of health information by public sector agencies and private organisations. The HPPs regulate the:

- collection,
- storage,
- access,
- alteration,
- accuracy
- use,
- disclosure,
- identifiers and anonymity and
- transferals and linkage

of health information. These are at [Schedule 1 of the HRIPA](#) and are dealt with in more detail at points 10-14 and 18-23.

### 9.2 Exceptions to the HPPs

There are a number of exceptions to the HPPs which are noted within Schedule 1. These are addressed at points 10 -23 below.

9.3 The Privacy Commissioner has published 4 [statutory guidelines](#) which provide guidance on the application of exemptions. They are:-

- [Statutory Guidelines on the Management of Health Services](#):- provide guidance on using and disclosing health information for the management of health services.
- [Statutory Guidelines on Training](#): provide guidance on using and disclosing health information for training purposes;
- [Statutory Guidelines on Research](#):- provide guidance on using and disclosing health information for research purposes;
- [Statutory Guidelines on the Collection of Health Information from a Third Party](#):- provide guidance on collecting health information about a person from a third party and on notifying a person when their health information has been collected from a third party.

A [Fact Sheet](#) explaining each of these guidelines is available on the website of the Office of the Privacy Commissioner.

9.4 The HRIPA allows the Privacy Commissioner to make Public Interest Directions to waive or modify the requirement of a public sector agency to comply with a HPP. The current directions which impact on the functions of the Department are:

- [Direction relating to the Redfern Waterloo Case Coordination Project](#):- modifies collection, use and disclosure HPPs.

9.5 Compliance with some of the IPPs and HPPs may be satisfied if the Department can show that it has taken reasonable steps, having regard to the circumstances, to comply with a requirement. Factors which will determine whether reasonable steps have been taken in the circumstances may include:

- the sensitivity of the information,

- the possible use of the information,
- the context in which the information was obtained,
- the need to maintain the integrity of the information,
- the number of people who will have access to the information,
- financial and practical effects of strategies for compliance on the continued ability of the agency to perform its legitimate functions,
- the potential effects on the individual if the Department does not comply with the principle,
- the risk to Department if it does not comply with the principle.

9.6 The requirements of each IPP and HPP are set out below. Each IPP and HPP is followed by the exceptions and modifications that apply to the particular principle and the manner in which the Department complies with the principle. IPPs and HPPs 1-9 are similar in most respects and are addressed together.

### PART 3

#### 10. Collection of personal and health information

10.1 IPP 1 & HPP 1 ([section 8 PPIPA](#) and [clause 1 of Schedule 1 HRIPA](#))

10.1.1 The Department must only collect personal and health information by lawful means and for a lawful purpose directly related to its functions and activities and the information must be reasonably necessary for that purpose.

10.1.2 Compliance with IPP1 & HPP 1

- (i) The Department complies with legal requirements when collecting personal and health information. Other legislation that imposes restrictions on the manner in which information is collected includes:
  - the [Workplace Surveillance Act 2005](#) – it is an offence under this Act, in certain circumstances for an employer to use surveillance cameras in the workplace - [Legal Issues Bulletin No. 41](#) provides advice on the use of CCTV surveillance in schools, TAFE NSW institutes and Department offices.
  - the [Surveillance Devices Act 2007](#) – it is an offence under this Act to record a private conversation, in certain circumstances - Legal Issues Bulletin No. 35 provides information about this offence.
  - the [Crimes Act 1900 \(NSW\)](#) or [Commonwealth Criminal Code](#) - it is an offence, in certain circumstances to photograph and video individuals without their consent - [Legal Issues Bulletin No. 35](#) deals with the use of cameras and phones to capture images.
- (ii) The Department collects information for lawful purposes relating to its functions and activities. The functions and activities of the Department are set out in legislation governing the Department's operations. These include:
  - [Technical and Further Education Commission Act 1990](#),
  - [Education Act 1990](#)
  - [Children \(Education Care Services\) National Law NSW \(NSW\)](#)
  - [Commission for Children and Young People Act 1998](#)
  - [Sporting Venues Authorities Act 2008](#)
  - [Apprenticeship and Traineeship Act 2001](#)

- [Combat Sports Act 2008](#)
- [Youth Advisory Council Act 1989](#)

10.2 IPP2 & HPP3 ([section 9 PPIPA](#) and [clause 2 Schedule 1 HRIPA](#))

10.2.1 The Department must collect personal and health information directly from the individual to whom it relates unless:

- the individual has consented to collection of their information from the other person, or
- the information is collected from the parent or guardian of a child under 16 years of age, or
- In respect of **health information**, it is unreasonable or impracticable to do so.

10.2.2 Exceptions:

The Department is not required to comply with this principle when:

- the information is collected in connection with proceedings before a court or tribunal, or
- handling a complaint or other matter that could be referred or made to an investigative agency or has been referred from an investigative agency, or
- it is lawfully authorised or required not to comply or non-compliance is implied under an Act or other law, or
- compliance would prejudice the interests of the individual to whom the information relates, or
- in respect of **health information**, when complying with the Privacy Commissioner's [Statutory Guidelines on the Collection of Health Information from a Third Party](#)

10.2.3 Modifications:

The Department may depart from this principle in respect of **personal information** when:

- compliance may detrimentally affect or prevent the proper exercise of its complaint handling or investigative functions, or
- collecting information about a student enrolled at a government school from the student's parent, guardian or caregiver, or
- collecting information about a student from other students or staff where it is necessary to promote and maintain a safe and disciplined learning environment,

10.2.4 Compliance with IPP2 and HPP3

- The Department collects personal and health information directly from current and prospective students and employees, other stakeholders and members of the public by a number of means including forms (paper and electronic), email, letter, telephone or the Department's websites.
- The Department may collect personal and health information about an individual from a third party if consent is given by the individual to whom the information relates or it is permitted under an Act. Acts that allow the Department to collect information from third parties include:

- Chapter 16A of the [Children and Young Persons Care and Protection Act 1998](#) which permits exchange of information to facilitate the provision of services to children and young persons by agencies that have responsibilities relating to the safety, welfare or wellbeing of children and young persons.
  - Part 5A of the [Education Act 1990](#) allows the Department to obtain information about a student to assist in assessing whether the enrolment of a particular student at a school is likely to constitute a risk to the health or safety of any person, including the student, and to develop and maintain strategies to eliminate or minimise any such risk. [Management of Health and Safety Risks Posed by a Student's Violent Behaviour - Guidelines](#) issued under Part 5A.
  - The [Work Health and Safety Act 2011](#) imposes certain obligations on the Department to secure the health and safety of workers and workplaces. The Department may collect information from a third party for purposes relating to its obligations to protect workers and other persons against harm to their health, safety and welfare.
- (iii) The Department of Education and Training [Privacy Code of Practice](#) allows for the collection of personal information from the parent or caregiver of a student over 16 years of age in particular circumstances and in consideration of relevant factors such as the student's maturity, family circumstances and what is in the best interests of the student. [Legal Issues Bulletin No.53](#) deals with the capacity of students under 18 years of age to make their own decisions when living independently.
- (iv) The Department may collect **health information** from an authorised representative when the individual is incapable of acting as permitted or required by HRIPA. A person lacks capacity if incapable by reason of age, injury, illness, physical or mental impairment of understanding the general nature and effect of the act, or communicating his/her intentions with respect to the HRIPA.
- (v) The [Statutory Guidelines on the Collection of Health Information from a Third Party](#) provide guidance when collecting health information from a person other than the person to whom the information relates.

10.3 IPP3 & HPP4 ([section 10 PPIPA](#) and [clause 4 Schedule 1 HRIPA](#)).

- 10.3.1 When collecting information from an individual the Department must take all steps that are reasonable in the circumstances to ensure that before the information is collected or as soon as practicable after collection, the individual to whom the information relates is made aware of:
- (i) the information is being collected,
  - (ii) the purposes for which it is being collected,
  - (iii) the intended recipients of the information,
  - (iv) whether the information is required by law or is voluntary,
  - (v) consequences to the individual if the information or part of it is not provided,
  - (vi) right of access to and correction of the information; and
  - (vii) name and address of agency collecting the information and the agency that is to hold it.

### 10.3.2 Exceptions

The Department is not required to comply with this principle when:

- (i) the information is collected for law enforcement purposes, or
- (ii) it is lawfully authorised or required not to comply or non-compliance is implied under an Act or other law, or
- (iii) compliance would prejudice the interests of the individual to whom it relates, or
- (iv) the individual to whom the information relates has consented, or
- (v) in respect of **health information**, complying with [Statutory Guidelines on the Collection of Health Information from a Third Party](#).

### 10.3.3 Modifications

The Department may depart from this principle in respect of **personal information** where:

- (i) compliance may detrimentally affect or prevent the proper exercise of its complaint handling or investigative functions, or
- (ii) it collects a student's information from the student's parent/carer and that person is made aware of the requirements in this section, or
- (iii) the parent/carer of a student enrolled in a government school has consented to the department not complying with the principle in respect of the student's information, or
- (vi) it is considered necessary to promote and maintain a safe and disciplined learning environment.

### 10.3.4 Compliance with IPP3 & HPP4

- (i) When collecting personal and health information the Department will take reasonable steps to inform the person to whom the information relates of the matters in IPP3 and HPP4. In most instances this is achieved by providing a collection notice at the time of collection. The form of wording will differ depending on the proposed use and disclosure of the information collected. A sample form of words for a collection notice is available at the Department's [privacy intranet site](#). When telephone conversations are monitored by recording for quality control and supervision purposes, clients will be advised of this at the outset of the conversation.

## 10.4 IPP4 and HPP2 ([section 11 of the PPIPA](#) and [clause 2 of Schedule 1](#) of the HRIPA)

10.4.1 When collecting information from an individual the Department must take steps that are reasonable in the circumstances (having regard to the purposes for which the information is collected) to ensure that:

- (i) the information is relevant to that purpose, is not excessive and is accurate, up to date and complete, and
- (ii) the collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

### 10.4.2 Compliance with IPP4 and HPP2

- (i) Business units that collect information will implement procedures to ensure the information they hold is kept up to date and relevant.



10.4.3 Unsolicited information is not “collected” for the purposes of the PPIPA and HRIPA and therefore is not subject to the requirements of the collection IPPs and HPPs.

## 11. Retention and security of personal and health information

11.1 IPP5 and HPP5 ([section 12 of the PPIPA](#) and [clause 5 of Schedule 1](#) of the HRIPA)

11.2 The Department must ensure that the personal and health information it holds:

- (i) is not kept for longer than necessary for the purposes for which it may lawfully be used, and
- (ii) is disposed of securely and in accordance with any requirements for the retention and disposal of this information, and
- (iii) is protected by taking reasonable security safeguards in the circumstances against loss, unauthorised access, use, modification or disclosure and against all other misuse, and
- (iv) when given to a person in connection with the provision of a service to the Department, everything reasonably within the Department’s power is done to prevent unauthorised use or disclosure of the information.

11.3 Exceptions

The Department is not required to comply with this principle in respect of **health information** when:

- (i) lawfully authorised or required not to comply or non-compliance is otherwise permitted, necessarily implied or reasonably contemplated under another Act or law.

11.4 Modifications

The Department may depart from this principle in respect of **personal information** where:

- (i) compliance may detrimentally affect or prevent the proper exercise of the Department’s complaint handling or investigative functions.

11.5 Compliance with the retention and security IPP & HPP.

- (i) The Department is committed to ensuring an appropriate level of security is applied to protect the confidentiality, integrity and availability of its information. All departmental information assets in electronic, paper, audio or video form, whether located in schools, institutes, corporate units or other locations is to be secured according to the information’s level of sensitivity, criticality and risk.
- (ii) The Department is progressively implementing the Electronic Document Records Management System (TRIM) across all business units with the aim of achieving substantial compliance with State Record’s Standard on Digital Recordkeeping.
- (iii) The Department’s Information Security Management System (ISMS) applies to all information assets. It is a framework and methodology used to manage information security risks. It facilitates the protection of information by identifying and classifying critical and sensitive information as directed by the Enterprise Data Policy and the performance of risk assessments in accordance with the Enterprise Risk Management Policy.



- (iv) Relevant legislation, whole of Government and Departmental policies that support compliance with this principle are:
- *Digital Information Security Policy*: applies to all NSW Government Departments, Statutory Bodies and Shared Services Providers. It establishes the digital information security requirements for the NSW public sector including the requirement to have an information Security Management System that appropriately addresses all identified risks.
  - [NSW State Records Act 1998](#) mandates the protection measures, retention timeframes, access and destruction provisions to be applied to state records.
  - *Records Management Program* is a set of policies, procedures and systems to manage its records in compliance with the State Records legislation and in accordance with the Department's business needs.
  - *Enterprise Data Policy* and implementation documents aim to promote data quality, increase accuracy of data used for decision making, improve data security including stakeholder data held by the Department and promote compliance with applicable laws.
  - *Enterprise Risk Management in the Department of Education and Communities Policy and accompanying Guidelines* embed enterprise risk management into all department processes including management of information held by the Department.
  - *Information Security Policy and Guideline* apply to all Department staff who access and use the Department's information assets in any form, this includes information held and maintained by the Department for other government agencies or private entities and information held and maintained for the Department by external parties.
  - *Communication Devices and Associated Services Policy and Guidelines* deal with the responsibilities of staff in relation to the use of departmental communication devices and associated services including telephones, mobile phones, computers, personal digital assistants, facsimiles, internet, intranet, email and broadband data services and inform staff about surveillance and monitoring of its computer systems and mobile communications to ensure security, integrity, efficiency and effectiveness of resources.
  - *Code of Conduct Policy and Procedures* require staff to comply with *the Employer Communication Devices Acceptable Use Guidelines*, its Records Management Procedures, the *State Records Act 1998* and privacy legislation.
  - *Business Continuity Management Policy* encourages business units that perform a critical business function to develop and implement a Business Continuity Plan (BCP) to manage the effects of severe unexpected events that impact the continuity of the Department's operations eg the release or loss of information such as student tax file numbers or staff addresses. It is not anticipated that BCPs be developed at school or college level as it is expected that they should be adequately covered by emergency response plans and higher level BCPs.

## 12. Access to personal and health information

12.1 IPPs 6 and 7 and HPPs 6 and 7 ([sections 13 and 14 of the PPIPA](#) and [clauses 6 and 7 of Schedule 1 of the HRIPA](#))

12.2 If the Department holds personal and health information it must take reasonable steps in the circumstances to enable a person to ascertain:

- (i) whether it holds personal information and
- (ii) whether it holds personal information relating to that person and
- (iii) if it holds personal information relating to that person:
  - the nature of the information, and
  - the main purposes for which the information is used; and
  - the individual's entitlement to gain access to the information.

12.3 If the Department holds personal or health information, it must at the request of the individual to whom the information relates, and without excessive delay or expense provide the individual with access to the information.

12.4 Exceptions

The Department is not required to comply with these principles when:

- (i) lawfully authorised or required not to comply or non-compliance is otherwise permitted or necessarily implied or reasonably contemplated under an Act or law.

12.5 Modifications

The Department may depart from these principles in relation to **personal information** to:

- (i) preserve the confidentiality of counsellor records, or
- (ii) preserve the confidentiality of information provided by staff or students about another student in circumstances where it is considered necessary to promote and maintain a safe and disciplined learning environment, or
- (iii) deny access when it might detrimentally affect or prevent the proper exercise of the Department's complaint handling or investigative functions, or
- (iv) allow the Department to obtain approval from the parent or caregiver of a student before releasing information about the student.

12.6 Compliance with the Access IPPs and HPPs

- (i) The Department will, at the request of an individual whose personal or health information it holds, provide the individual with access to their information.
- (ii) Where practicable, individuals are informed of the right to access their personal and health information by way of a notice at the time of collection.
- (iii) Individuals wishing to exercise their right to access their own personal or health information should apply in writing or direct their inquiries to the business unit with responsibility for the information or the Legal Services Directorate if the business unit is not known. A written request form for access to personal/health information is at [Annexure 1](#).
- (iv) Requests for access are usually handled by the relevant business unit, in accordance with the [Procedures for Access to Personal and Health Information](#), published on the privacy intranet site. The procedures provide that:
  - A request for access to information must clearly identify the information to which it refers.

- Factors to consider when deciding to require a fee to provide access to information. These may include:
    - the volume of documents requested, and
    - whether the documents have previously been provided to the individual.
  - Access may be granted by providing a copy of the information or allowing the individual to read the information without uplifting it.
  - If access is denied, the Department will provide the individual with reasons for this decision and information about his/her right to make an application for internal review of the decision.
- (v) Individuals can also access information under the [Government Information \(Public Access\) Act 2009](#) (GIPAA). Details of these procedures are available from the Department [Information Access Unit](#).
- (vi) Nothing in the [PPIPA](#) or [HRIPA](#) affects the operation of the [GIPAA](#). Provisions within the GIPAA that impose conditions or limitations on an individual's access to information under that Act are not affected by the PPIPA and apply in the same way to a request for access under the PPIPA.
- (vii) Access to personal and health information held by the Department may also be available under the [State Records Act 1998](#).

### 13. Alteration of personal and health information

13.1 IPP 8 and HPP 8 ([section 15 of the PPIPA](#) and [clause 8 of schedule 1 of the HRIPA](#))

13.2 The Department must amend personal and health information it holds on an individual at the request of the individual to:

- (i) Ensure the information is accurate and, having regard for the purpose the information was collected, is relevant, up to date, complete and not misleading.
- (ii) When the Department is not prepared to amend the information as requested, it must, if so requested, take reasonable steps to attach to the information, in a way capable of being read with it, a statement provided by the individual of the amendment sought.
- (iii) When the Department amends an individual's information the individual is entitled to have recipients of the information notified of the amendments if it is reasonably practicable.

13.3 Exceptions

The Department is not required to comply with this principle when;

- (i) It is lawfully authorised not to comply or non-compliance is permitted, implied or contemplated under an Act or any other law.

13.4 Modifications

The Department may depart from this principle in relation to **personal information**:

- (i) to maintain confidentiality of counsellor records, or
- (ii) if compliance might detrimentally affect or prevent the proper exercise of the Department's complaint handling or investigative functions, or
- (iii) to amend personal information held on a student at the request of the student's parent or caregiver, or
- (iv) to preserve the confidentiality of information about a student in circumstances where it is considered necessary to promote and maintain a safe and disciplined learning environment.

### 13.5 Compliance with the Alteration IPP and HPP

- (i) The Department will take reasonable steps to ensure that individuals are informed of their right to request amendment of their personal and health information by way of a notice at the time of collection.
- (ii) An individual can request amendment of his/her personal or health information held by the Department by contacting the business unit where the information is held or the Legal Services Directorate if the business unit is not known.
- (iii) A request should be in writing identifying the information involved, the document on which it is recorded, the changes requested, the document/s on which the information is recorded and evidence in support of the need for amendment. A written request for amendment of personal or health information is at [Annexure 2](#).
- (iv) Requests are dealt with by the business unit where the records are held, in accordance with the [Procedures for Alteration of Personal and Health Information](#) published on the privacy intranet site.  
The procedures provide that:
  - A request for amendment of information must clearly identify the information involved and the amendment sought.
  - Factors to consider when deciding whether to make the amendment requested.
  - Factors to consider when determining what are reasonable steps to be taken to attach a statement of the amendment sought to the information.
  - Factors for consideration when determining what is reasonably practicable when notify recipients of the information about any amendment.
- (v) Nothing in the [PPIPA](#) or [HRIPA](#) affects the operation of the [GIPAA](#) in respect of amendment of information. Provisions within the GIPAA that impose conditions or limitations on amendment of an individual's information under that Act are not affected by the PPIPA and apply in the same way to a request for amendment under the PPIPA.

## 14. Accuracy of personal and health information

### 14.1 IPP 9 and HPP 9 ([section 16 of the PPIPA](#) and [clause 9 of schedule 1 of the HRIPA](#))

14.2 Before using personal or health information which it holds the Department must take reasonable steps in the circumstances to ensure that, having regard to the purpose for which it is to be used the information is relevant, up to date, complete and not misleading.

### 14.3 Compliance with the Accuracy IPP and HPP

- (i) In general terms 'use' refers to action taken by the Department when applying information for its own purposes and involves actions within the Department rather than those with external persons or bodies.
- (ii) The Department informs individuals of their right to access and amend their personal and health information at the time of collection. Requests to update the information are generally made by the business unit holding the information. The frequency with which these requests are made will be governed by a number of factors including the nature of the information held, its intended use and the ease with which it can be amended.

## 15. Use of Personal Information

15.1 IPP 10 ([section 17 of the PPIPA](#)).

15.2 The Department must not use personal information it holds for a purpose other than that for which it was collected unless:

- (i) the individual consents to his/her information being used in that way, or
- (ii) it is to be used for a purpose directly related to the purpose for which it was collected, or
- (iii) the other purpose for which the information is to be used is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual to whom the information relates or of another person.

15.3 Exceptions

The Department is not required to comply with this principle if:

- (i) the other purpose is reasonably necessary for law enforcement purposes or for the protection of the public revenue, or
- (ii) it is lawfully required not to comply or non-compliance is permitted, implied or contemplated under an Act or other law.

15.4 Modifications

The Department may depart from this principle in relation to personal information:

- (i) to use information for the purpose of child protection, or
- (ii) if it is reasonably necessary in order to enable the Department to exercise its complaint handling or investigative functions,
- (iii) to obtain the consent of a parent, guardian or caregiver of a student enrolled at a government school to use the student's information for a purpose other than that for which it was collected, or
- (iv) if it is considered necessary to promote and maintain a safe and disciplined learning environment, or
- (v) to use information for the purpose of obtaining legal advice and representation or for use in legal proceedings.

15.5 Compliance with the Use IPP

- (i) In most situations, the Department obtains consent to use an individual's personal information for specified purposes at the time of collection, for example on school and TAFE student enrolment forms.
- (ii) Where personal information is stored in a digital storage system, business units will ensure that appropriate descriptions are used to avoid errors or misinterpretation which may result in misuse of the information. Uniform description of information also facilitates its transfer between business centres. These issues are addressed in the Department's policies and procedures and the [Guide to Labelling Sensitive Information](#) which applies to all NSW Departments.
- (iii) Personal information that has not been obtained through a formal collection process but is created from collating known information about an individual e.g. records created by schools and Institutes of student results or records of employee training, should only be used for the purpose/s for which the Department has created and holds the information.

## 16. Disclosure of Personal Information

### 16.1 IPP 11 ([section 18 of the PPIPA](#)).

The Department must not disclose personal information to any person or body other than the person to whom it relates unless:

- (i) The disclosure is directly related to the purpose for which the information was collected and the Department has no reason to believe the person would object to the disclosure, or
- (ii) The individual concerned is reasonably likely to have been aware or was made aware that information of this type was usually disclosed to that other person or body, or
- (iii) The Department believes, on reasonable grounds, that the disclosure is necessary to prevent or lessen serious and imminent threat to life or health of the individual or other person.

If personal information is disclosed to another person or body that is a public sector agency that other agency must not use or disclose the information for a purpose other than the purpose for which the information was provided.

### 16.2 Exceptions

The Department is not required to comply with this principle where:

- (i) the disclosure is made in connection with proceedings for an offence or for law enforcement purposes, or
- (ii) the disclosure is to a law enforcement agency to locate a missing person, or
- (iii) the disclosure is authorised by a subpoena, search warrant or statutory instrument, or
- (iv) disclosure is reasonably necessary for the protection of public revenue, or
- (v) disclosure is reasonably necessary to investigate an offence where there are reasonable grounds to believe an offence has been committed, or
- (vi) the information is disclosed to an investigative agency, or
- (vii) it is lawfully authorised or required not to comply or non-compliance is permitted, implied or contemplated under an Act or any other law, or
- (viii) the individual to whom the information relates consents to the Department not complying, or
- (ix) the principle does not prevent or restrict disclosure to other public sector agencies administered by the same Minister to inform the Minister about a matter under that administration or to an agency administered by the Premier to inform the Premier.

### 16.3 Modifications

The Department may depart from this principle where:

- (i) the disclosure is for child protection purposes, or
- (ii) compliance might detrimentally affect or prevent the exercise of its complaint handling and investigative functions, or
- (iii) to allow for consideration of any objection from a parent or caregiver of a student before disclosing information about the student, or
- (iv) it is in the best interests of a student to disclose the student's information to their parent or caregiver, or
- (v) to obtain the consent of a parent or caregiver to use a student's information for a purpose other than the purpose for which it was collected.



## 16.4 Compliance with the Disclosure IPP

- (i) The Department will notify individuals of the anticipated recipients of their information at the time of collection, for example TAFE students are notified at enrolment that student information collected during their enrolment may be disclosed to other State and Commonwealth agencies and, in the case of a student undertaking an apprenticeship, certain information will be provided to employers.
- (ii) Business Unit managers are requested to regularly update information they hold so it reflects the individual's current situation. The frequency of updating information and the manner in which this is done will depend on the circumstances and the information involved. For example, principals are reminded annually to renew consent from parent/caregivers for publication of their child's personal information. A template letter for seeking consent from parents is provided in [Privacy Bulletin No. 9](#)
- (iii) The Department may disclose personal information for the purpose of research by external bodies. Research undertaken in NSW Government schools or pre-schools when the researcher interacts with students or staff is undertaken in compliance with the [State Education Research Approvals Process and Guidelines \(SERAP\)](#). The guidelines require informed consent of the student or his/her parent/caregiver for participation in a research project. Research involving TAFE NSW is conducted in accordance with the [Guidelines for Applications to Conduct Research in TAFE NSW](#), modelled on SERAP.
- (iv) Requests for personal information for research, data linkage and evaluation and review of programs associated with funding allocations will be handled with reference to the Privacy Commissioner's Direction on Disclosures of Information by Public Sector Agencies for Research Purposes which enable the Department to disclose personal information for research where this would otherwise breach IPP 11 or IPP 12, if the research complies with certain requirements. These include a requirement that the research has been approved by a committee established for the purpose of giving ethical approval to research projects after the committee has considered the privacy implications of the collection and subsequent use of such information by the researcher in the absence of express consent.
- (v) A Department working party is currently developing a whole of department position on data sharing and linkage of personal information held by the Department.
- (vi) The Department is required by law to disclose personal information to various State and Commonwealth government agencies. These include requests for information:
  - concerning the safety, welfare or wellbeing of a child or young person under the [Children and Young Persons \(Care and Protection\) Act 1998](#).
  - about an individual to determine his/her eligibility to receive benefits under the [Social Security \(Administration\) Act 1999 \(Cth\)](#).
  - relating to ascertaining the identity or whereabouts of a person believed to be a non-citizen, under the [Migration Act 1958 \(Cth\)](#) about a child's location in connection with a location order issued under the [Family Law Act 1975](#).
  - relating to the disclosure of corrupt conduct or maladministration under the [Public Interest Disclosures Act 1994](#).
- (vii) In response to a request made under an Act the Department will only provide the information requested and which falls within the scope of what

can lawfully be obtained. [Legal Issues Bulletin No. 47 and 50](#) address exchange of information with other government agencies.

- (viii) The Department must produce documents requested under subpoena. [Legal Issues Bulletin No. 25](#) deals with return of a subpoena to produce.
- (ix) The Department has an enforcement role with respect to the compulsory schooling duty of parents under the [Education Act 1990](#) and the operation of care services under the [Children \(Education and Care Services\) National Law \(NSW\)](#). The Department may disclose personal information when meeting its obligations under these Acts.
- (x) Where the Department is required to disclose personal information to a law enforcement agency it will first establish the purpose for which the information is required and only provide information relating directly to that purpose. The Department has a [Memorandum of Understanding with NSW Police](#) which deals with the exchange of information with that agency. Exchange must be made in accordance with the PPIPA.

## 17. Special Restrictions on Disclosure of personal information

### 17.1 IPP 12 ([section 19 of the PPIPA](#))

- (i) The Department must not disclose personal information relating to an individual's ethnic or racial origin, political opinions, religious and 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 another person.
- (ii) The Department must not disclose personal information to a person or body in a jurisdiction outside New South Wales or to a Commonwealth agency unless a relevant privacy law that applies to the personal information concerned is in force in that jurisdiction, or the disclosure is permitted under a privacy code of practice.

### 17.2 Exceptions

The Department is not required to comply with this principle where:

- (i) it is reasonably necessary for the purposes of law enforcement in circumstances where there are reasonable grounds to believe that an offence may have been or may be committed, or
- (ii) it is lawfully authorised or required not to comply or non-compliance is permitted, implied or reasonably contemplated under an Act or any other law, or
- (iii) if the individual to whom the information relates has consented, or
- (iv) disclosure is to another public sector agency administered by the same Minister for the purpose of informing the Minister about a matter under that administration, or to an agency administered by the Premier for the purpose of informing the Premier.

### 17.3 Modifications

The Department may depart from this principle:

- (i) for the purpose of child protection, or
- (ii) if compliance might detrimentally affect or prevent the proper exercise of the Department's complaint handling or investigative functions, or
- (iii) to disclose the information of a student enrolled at a government school to the student's parent or caregiver (with the exception of counsellor records), or



- (iv) if the parent or caregiver of a student to whom the information relates expressly consents to the Department not complying, or
- (v) where it is considered necessary to promote and maintain a safe and disciplined learning environment, or
- (vi) to use information for the purpose of obtaining legal advice and representation or for use in legal proceedings.

#### 17.4 Compliance with Special Restrictions on Disclosure

- (i) Requests for information for the purposes of research, evaluation, data linkage and program and funding review often involve information about a student's ethnic origin. These requests are dealt with as explained at 16.4(iv).
- (ii) The Privacy Commissioner has published a draft Privacy Code of Practice for Disclosures of Personal Information Outside New South Wales. The proposed Code addresses the disclosure of personal information, including sensitive information to Commonwealth, State and Territory education and training agencies and bodies for various purposes. When the Code of Practice becomes operational staff will be informed by a feature article on "Our Intranet".

### 18. Use and Disclosure of Health Information

#### 18.1 HPPs 10 & 11 ([Schedule 1 clauses 10 & 11 HRIPA](#))

The Department must not use or disclose health information for a purpose other than the purpose for which it was collected **unless**:

- (i) the individual has consented to the use or disclosure for the other or secondary purpose, or
- (ii) the secondary purpose is directly related to the primary purpose and the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose, or
- (iii) The Department reasonably believes the use or disclosure is necessary to lessen or prevent a serious and imminent threat to the life, health or safety of the individual or another person or a serious threat to public health or public safety, or
- (iv) it is reasonably necessary for the funding, management, planning or evaluation of health services, or
- (v) it is reasonably necessary for:
  - o training employees,
  - o research, or
  - o the compilation or analysis of statistics
 in the public interest, where de-identified information cannot be used and it is impracticable to obtain the consent of the individual. If the information could identify an individual it is not to be published in a generally available publication, and the use of the information is in accordance with any guidelines published by the Privacy Commissioner, or
- (vi) it is used by a law enforcement agency to ascertain the whereabouts of an individual who has been reported to a police officer as a missing person, or
- (vii) the Department has reasonable grounds to suspect that unlawful activity has been or may be engaged in, or
- (viii) a Department employee has or may have engaged in conduct that may be grounds for disciplinary action, or
- (ix) it is reasonably necessary for the exercise of law enforcement functions by a law enforcement agency in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed, or

- (x) it is reasonably necessary for the complaint handling functions or investigative functions by investigative agencies, or
- (xi) the Department or an employee is handling a complaint or other matter that could be referred or made to an investigative agency, or
- (xii) the Department is lawfully authorised or required not to comply with the provision or non-compliance is otherwise permitted, implied or contemplated under an Act or any other law, or
- (xiii) disclosure is to another public sector agency under the administration of the same Minister for the purposes of informing that Minister about any matter within that administration, or
- (xiv) disclosure is to any public sector agency under the administration of the Premier for the purposes of informing the Premier about any matter.

## 18.2 Compliance with the Use and Disclosure HPPs

- (i) The Department obtains consent for the use and disclosure of an individual's health information at the point of collection for example the Application for approval to undertake the equivalent of Year 10 of secondary education at TAFE NSW requires students to provide permission to the Principal of their school to release their information and records to be used in determining whether permission is granted for the student to enter a TAFE Year 10 equivalent program. This information may include the student's health information.
- (ii) Legislation that may require the Department to disclose an individual's health information includes [Workplace Injury Management and Workers Compensation Act 1998](#), in the management of employees' health in the workplace, [Children and Young Person's Care and Protection Act](#), in respect of matters concerning children and young persons' safety, welfare or wellbeing, [Teaching Service Act 1980](#), when managing employee conduct and performance issues, [Technical and Further Education Commission Act 1990](#) when dealing with fitness and capacity to work.
- (iii) The Department may use and disclose an individual's health information without consent in accordance with the Privacy Commissioner's Statutory Guidelines on the Management of Health Services. The Guidelines address use and disclosure for funding, management, planning and evaluation of health services, what are reasonable steps to de-identify health information, the practicality of obtaining consent and what to consider when using and disclosing de-identified health information.
- (iv) Where the Department discloses health information for research, data linkage, evaluation and review of programs and funding allocations without the consent of the person to whom the information relates, in accordance with the [Privacy Commissioner's Statutory Guidelines on Research](#). These address the conditions upon which the Department can rely when applying the research exemption for the collection, use and disclosure of health information.

## 19. Identifiers in relation to health information

### 19.1 HPP 12 ([Schedule 1 clause 12 HRIPA](#))

The Department may only assign identifiers to individuals and use and disclose them, if reasonably necessary to enable it to carry out its functions efficiently. If it is necessary for a private sector agency to use or disclose an identifier which the Department has assigned to an individual in order to fulfil its obligations to the Department, the private sector agency may adopt as its own or use or disclose the identifier assigned by the Department.

## 20. Anonymity and health information

### 20.1 HPP 13 ([Schedule 1 clause 13 HRIPA](#))

Where it is lawful and practicable, the Department will give individuals the opportunity to not identify themselves when receiving health services from the Department.

## 21. Transborder data flows and data flow to the Commonwealth of health information

### 21.1 HPP 14 ([Schedule 1 clause 14 HRIPA](#))

The Department cannot transfer health information to a person or body outside NSW or to a Commonwealth agency **unless**

- (i) the Department reasonably believes the recipient is subject to a law, binding scheme or contract that effectively upholds principles of fair handling of information that are substantially similar to the HPPs, or
- (ii) the individual consents to the transfer, or
- (iii) the transfer is necessary for the performance of a contract between the individual and the Department, or for implementation of pre-contractual measures taken in response to the individual's request, or
- (iv) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party, or the transfer is for the benefit of the individual and it is impracticable to obtain the individual's consent and the individual would be likely to give consent, or
- (v) the Department reasonably believes the transfer is necessary to lessen or prevent a serious and imminent threat to the life, health and safety of the individual or other person or a serious threat to public health or safety, and
- (vi) the Department has taken reasonable steps to ensure that the transferred health information will not be held, used or disclosed by the recipient inconsistently with the NSW HPPs, or
- (vii) the transfer is permitted or required under law.

## 22. Linkage of health information

### 22.1 HPP 15 ([Schedule 1 clause 15 HRIPA](#))

The Department must not:

- (i) include health information about an individual or an identifier of an individual in a state or national health records linkage system without the individual's express consent.

## 22.2 Exceptions

The Department is not required to comply with this principle if:

- (i) lawfully authorised or required not to comply, or
- (ii) non-compliance is permitted, implied or contemplated under an Act, or
- (iii) the use and disclosure is for research purposes or compilation of analysis or statistics in compliance with HPPs 10 and 11.

## 23. Compliance with identifiers, anonymity, transborder data flow and linkage principles

- (i) The Department will comply with the transborder and linkage principles unless lawfully authorised not to comply for example, disclosure of data under the [Australian Bureau of Statistics Act 1975](#).

## PART 4

### 24. Complaints - Internal and External Review

#### Who can apply for an internal review?

- 24.1 A person who is aggrieved by the way in which the Department has handled their personal or health information may either make a complaint to the Privacy Commissioner or apply to the Department for an internal review of that conduct.
- 24.2 Complaints to the Privacy Commissioner are dealt with under [Part 4 Division 3 of the PPIPA](#) and internal reviews by public sector agencies are handled under [Part 5 of the PPIPA](#).
- 24.3 An application for internal review should identify conduct by the Department which an individual believes amounts to:
  - a breach of an IPP or HPP; or
  - a breach of a Code of Practice that applies to the Department; or
  - an inappropriate disclosure by the Department of personal or health information kept in a public register.
- 24.4 An aggrieved person is usually the person who is the subject of the personal or health information at issue. In certain circumstances it may include a person other than the subject of the information if that person has been specifically and adversely affected by the alleged breach. The question of whether a person is aggrieved will depend on the facts of the case.
- 24.5 Where a person lacks capacity, by reason of age, injury, illness physical or mental impairment, to understand the general nature and effect of the PPIPA or HRIPA or is unable to communicate his/her intentions with respect to them an authorised representative may act on the individual's behalf.
- 24.6 If a person wishes to act on behalf of an applicant not lacking capacity consideration will be given to the reasons for this and the applicant may be required to complete an Authority Form.

#### How to make an application for internal review

- 24.7 An application for internal review must:
  - be in writing;

- be addressed to the Department;
- specify an address in Australia to which the Department can send notification of the outcome of the internal review; and
- be lodged with the Department within 6 months from the time the applicant first became aware of the conduct the subject of the application or such later date as the agency allows.

24.8 A [Privacy Internal Review Application Form](#) can be obtained from the Department's website and intranet, by writing to:

Legal Services Directorate,  
Department of Education and Communities,  
GPO Box 33 Sydney NSW 2001

or by emailing [legal@det.nsw.edu.au](mailto:legal@det.nsw.edu.au).

### How are internal reviews conducted?

24.9 Applications for internal review are handled by the Legal Services Directorate with reference to guidance material issued by the Information and Privacy Commission including the Privacy Commissioner's checklist for agencies. A practice note for use by Legal Officers conducting internal reviews requires that a copy of the Privacy Commissioner's checklist for agencies be completed and officers consult with applicants when conducting internal reviews.

24.10 When an application is received it is allocated to a reviewing officer with the delegation to determine whether the Department has acted in breach of privacy legislation. The reviewing officer may refer the matter to another officer within the Directorate to assess and, if appropriate, conduct a fact finding investigation.

24.11 If the application is assessed as meeting the requirements identified at 24.3 and 24.7 above, the legal officer will notify the Privacy Commissioner of the application and inform the applicant in writing of:

- the Department's decision to conduct an internal review,
- the name, position and contact details of the officer/s handling the matter,
- the Department's understanding of the conduct complained about and the IPPs and/or HPPs at issue,
- the independence of officer/s handling the internal review,
- the required completion date for the internal review (60 days from the date the application was received),
- the applicant's right to apply for external review by the [NSW Civil and Administrative Tribunal](#) if the review is not completed within 60 days from receipt,
- that the applicant and Privacy Commissioner will be kept informed of the progress and findings of the review,
- the range of actions the department may take in resolving the complaint which include:
  - take no action,
  - make a formal apology,
  - take appropriate remedial action which may include payment of compensation,
  - implement measures to prevent recurrence of the conduct.

- 24.12 The legal officer conducting the investigation will follow the Practice Note for Conducting an Internal Review, which requires the officer to:
- assist the applicant to provide all relevant information and documentation in support of the complaint, including the particulars and evidence of the alleged breach and the harm, if any, caused by the alleged breach,
  - interview relevant staff and examine records and obtain any other pertinent information on the circumstances of the alleged breach,
  - prepare a report setting out the steps taken in the investigation, the conclusions reached and recommendation for action to be taken to resolve the complaint,
  - refer the fact finding report to the Privacy Commissioner, for submissions and to the determining officer for consideration when making the determination, and
  - consult with the applicant during the course of the investigation.
- 24.13 The Practice Note for Conducting an Internal Review requires the determining officer to:
- consider the fact finding report and any submissions from the Privacy Commissioner when determining whether a breach has occurred,
  - consult with the applicant about the complaint if further information is required and provide the applicant with the estimated time of completion of the internal review. A review must be conducted as soon as is reasonably practicable and if it is not completed within 60 days an applicant can apply to the NSW Civil and Administrative Tribunal for external review,
  - write to the applicant and Privacy Commissioner without unreasonable delay informing them of:
    - the findings of the review and reasons for the findings;
    - the action proposed to be taken and reasons for that action; and
    - the applicant's right to have the findings and reasons for the findings reviewed by the NSW Civil and Administrative Decisions Tribunal.
- 24.14 On reviewing the conduct of a Government department the [NSW Civil and Administrative Tribunal](#) may make orders requiring the Department to:
- refrain from conduct or action which breaches an IPP or HPP or privacy code of practice,
  - perform in compliance with an IPP or HPP or Privacy Code of Practice,
  - correct information disclosed by the Department,
  - take specified steps to remedy loss or damage suffered,
  - refrain from disclosing information in a public register,
  - pay damages of up to \$40,000 for loss or damage suffered where the applicant has suffered financial loss or psychological or physical harm as a result of the conduct.

## PART 5

### 25. Legislation affecting the Department's processing of information includes:

[Privacy and Personal Information Protection Act 1998](#), identifies principles for the handling of personal information

[Health Records and Information Privacy Act 2002](#), identifies principles for the handling of health information.

[State Records Act 1998](#), provides for the creation, management and protection of the records of public offices of the State and for public access to those records.

[Government Information \(Public Access\) Act 2009](#), promotes open accountable, fair and effective government and ensures members of the public have the right to



access government information.

[Public Interest Disclosures Act 1994](#), encourages and facilitates the disclosure in the public interest of corrupt conduct, maladministration, serious and substantial waste and government information contravention in the public sector.

[Education Act 1990](#), allows the Department to obtain information about students from relevant agencies.

[Children and Young Persons \(Care and Protection\) Act 1998](#), provides for the exchange of information for child protection purposes between prescribed bodies.

**26. Policies affecting the Department's processing of information include:**

Digital Information Security Policy,  
Guide to Labelling Sensitive Information,  
Communication Devices & Associated Services Policy and Guidelines  
Enterprise Data Policy and information to support implementation  
Enterprise Risk Management in DEC Policy and Guidelines,  
Information Security Policy and Guidelines,  
Information Security Management System  
Records Management Program and Manual  
Social Media Policy and Guidelines  
Incident Reporting Policy and Procedures  
Code of Conduct Policy and Procedure  
Legal Issues Bulletins and Privacy Bulletins,  
Memorandum of Understanding between DET and NSW Police  
Protecting and Supporting Children and Young People Policy and Procedures  
Operational Guidelines between Child Wellbeing Units  
MOU regarding use and storage of information on WellNet  
Information Security Policy and Guideline–  
Online Communication Services: Acceptable Usage for School Students  
Student Counselling Files Policy – TAFE  
Release Student Information Policy - TAFE  
Release of Student Information Procedure – TAFE  
Apprenticeships and Traineeships Information Collection Procedure – TAFE  
Online Communication Services- Code of Expected User Behaviour - TAFE  
Online Communication Services – Acceptable Usage – TAFE  
Authority to Release Centrelink Information –TAFE  
Apprenticeship and Traineeships - Information Collection and Reporting Procedure –  
TAFE

## 27. Dissemination of Policies and Training

- 27.1 The Department maintains a privacy home page on its intranet site which is accessed through the Legal Services Directorate homepage. On this page are links to:
- Privacy Bulletins and Legal Services Bulletins addressing procedures and protocols in relation to the application of privacy principles to the Department's functions,
  - Department of Education and Training Privacy Code of Practice,
  - A video – Privacy in Focus - which highlights the application of privacy principles to the Department's functions,
  - Privacy legislation,
  - Office of the Privacy Commissioner
  - Application for internal review
  - Procedures for conducting an internal review and handling requests for access to and alteration of information.
- 27.2 The Department's [website](#) has links to the Information Privacy Commission, Department of Education and Training Privacy Code of Practice, Application for Internal Review and Privacy Bulletin No. 9 on Issues regarding the publication of material accessible by the general public. The website is continually being updated to include further information. All officers of the Legal Services Directorate provide telephone advice to staff via the Legal Services Directorate advisory service which operates from 9:00am – 5:00pm Monday to Friday.
- 27.3 All officers of the Legal Services Directorate provide targeted training to schools, TAFE institutes and corporate staff on their legal obligations and rights in various areas including privacy.
- 27.4 Updates and new initiatives in the application of privacy policies and procedures are published on the Department's intranet news page – SchoolBiz, which is published each week.
- 27.5 A web-based self-assessment survey on privacy will be issued annually to a random sample of schools, TAFE Colleges and principals' reference groups. It will consist of scenario based questions and will double as an assessment and training tool.
- 27.6 A reminder to principals to request parents/caregivers update or amend their consent for publication of their child's information will be published on School Biz within the first month of each school year. Privacy Bulletin No. 9 contains templates that schools can tailor to seek permission from parents.

## 28. Responsibilities

- 28.1 All legal officers in the Legal Services Directorate are responsible for disseminating information about privacy to Department staff and may conduct investigations as part of a privacy internal review.



- 28.2 A senior legal officer has oversight of privacy matters, is responsible for recording statistical information about privacy complaints for inclusion in the Department's Annual Report and to the Privacy Commissioner, coordinating responses to requests for legal advice on privacy matters, overseeing privacy information on the internet and intranet sites and liaising with the [Office of the Privacy Commissioner](#) about privacy matters.
- 28.3 The Director Legal Services, Chief Legal Officer, three Principal Legal Officers and Manager Information Access Unit have delegation to determine privacy complaints.
- 28.4 All staff are responsible for complying with the privacy legislation. Staff should be aware that Part 8 of both the [PPIPA](#) and [HRIPA](#) contain criminal offences for corrupt disclosure of personal and health information, and for offering to supply such information.

## 29. Contractual Arrangements

- 29.1 The Department has a range of contractual arrangements. Where such arrangements require the Department to disclose an individual's personal or health information it takes reasonable steps to ensure that the party with which it is contracting does not inappropriately use or disclose information by inserting clauses in the agreement requiring compliance with the PPIPA and HRIPA.

## PART 6 ANNEXURES

### Annexure 1

#### APPLICATION FOR ACCESS

Application under the *Privacy and Personal Information Protection Act 1998* and/or *Health Records and Information Privacy Act 2002* for access to the applicant's personal and/or health information.

#### Applicant details

Name ..... Title: Mr / Ms / other .....

(Full Name)

Postal address.....

State .....Post Code.....

Email (optional).....

#### Access and Cost

As the applicant, you have a right under the legislation to access personal or health information concerning yourself that is held by the Department of Education and Communities. You are entitled to have access without excessive delay or cost.

Access may be granted but limited to allowing you to view the documents only.

The Department may require you to pay a fee if the application request involves a considerable diversion of its resources.

The Department may refuse to process your application in part, or in whole, if there is an exemption under the legislation or a Code of Practice that restricts disclosure of the information sought.

You have a right to request an internal review by the Department, of a decision in relation to your application for access. A request for internal review can be sent to the address listed below.

#### Proof of Identity

When seeking access to your, your child's or another person's personal or health information on their behalf, you may be required to provide proof of identity. This requirement will be met by providing a copy of one of the following documents:

- Australian driver photo licence showing current address, or
- Current Australian passport, and current address details, or
- Other proof of name, signature, relationship to the person on whose behalf you are acting and current address details.

You will be advised by the person processing your application if proof of identity is required.

**Information requested**

I am seeking my own personal and/or health information.

I am seeking personal and/or health information about my child or person for whom I have legal guardianship.<sup>1</sup>

I am seeking personal and/or health information on behalf of another person other than my child.<sup>2</sup>

I am seeking information on behalf of another person other than my child for the following reason/s:

.....  
.....

I am seeking access to the following information held by the Department: [complete information on a separate page if necessary]

.....  
.....

I am seeking the above information for the period from .....to .....

**Where to send your application**

Your application can be submitted to the business centre holding the information or Legal Services Directorate: email: [legal@det.nsw.edu.au](mailto:legal@det.nsw.edu.au) or by mail to:

Legal Services Directorate  
Department of Education and Communities  
GPO Box 33  
Sydney NSW 2001

Further information about your application can also be obtained from these locations.

**Signature and declaration**

I declare that the information I have provided on this form is true and correct.

Signed .....Date ...../...../.....

**Privacy Notice**

*The information provided on this application form is being obtained for the purpose of processing your application for access to information. Providing this information is required by law. It will be stored securely. If you do not provide all or any of this information it could prevent or delay the processing of your application.*

<sup>1</sup> Please provide evidence of your relationship which the person whose personal information you are requesting if the Department does not already hold that information.

<sup>2</sup> If you are applying on behalf of another person other than your child or a person for whom you have legal guardianship please provide written authority and ID from that person.

## Annexure 2

### APPLICATION FOR ALTERATION

Application under the *Privacy and Personal Information Protection Act 1998* and/or *Health Records and Information Privacy Act 2002* for alteration of the applicant's personal and/or health information.

#### Applicant details

Name ..... Title: Mr / Ms / other .....

(Full Name)

Postal address.....

State .....Post Code.....

Email (optional).....

As an applicant you have a right under the legislation to request alteration of personal and/or health information concerning yourself that is held by the Department of Education and Communities, to ensure it is accurate and, having regard to the purpose for which it was collected, is relevant, up to date, complete and not misleading.

If the Department is not prepared to amend the information you may request that it attach to the information a statement of the amendment sought.

The Department may refuse to process your application in part or in whole if there is an exemption under the legislation or a Code of Practice that restricts the alteration sought.

You have a right to request an internal review by the Department, of a decision in relation to your application for alteration. A request for internal review can be sent to the address listed below.

#### Proof of Identity

When seeking alteration of your, your child's or another person's personal and/or health information you may be required to provide proof of identity. This requirement will be met by providing a copy of one of the following documents:

- Australian driver photo licence showing current address, or
- Current Australian passport, and current address details, or
- Other proof of name, signature, relationship to the person on whose behalf you are acting or current address details.

You will be advised by the person processing your application if proof of identity is required.

**Amendment requested**

- I am seeking amendment of my own personal and/or health information.
- I am seeking amendment of personal and/or health information about my child or person for whom I have legal guardianship.<sup>1</sup>
- I am seeking amendment of personal and/or health information on behalf of another person other than my child.<sup>2</sup>

I am seeking information on behalf of another person other than my child for the following reason/s: [complete information on a separate page if necessary]

.....  
.....

I am seeking the following amendments to information held by the Department:

.....  
.....

**Where to send your application**

Your application can be submitted to the business centre holding the information or Legal Services Directorate: email: [legal@det.nsw.edu.au](mailto:legal@det.nsw.edu.au) or by mail to:

Further information about your application can also be obtained from these locations.

Legal Services Directorate  
Department of Education and Communities  
GPO Box 33  
Sydney NSW 2001

You application can be lodged at the business centre that holds the personal or health information you wish to have amended or, if not known, to the address or email listed above.

**Signature and declaration**

I declare that the information I have provided on this form is true and correct.

Signed ..... Date ...../...../.....

**Privacy Notice**

*The information provided on this application form is being obtained for the purpose of processing your application for alteration of information. Providing this information is not required by law however if you do not provide all or any of this information it could prevent or delay the processing of your application. It will be stored securely.*

<sup>1</sup> Please provide evidence of your relationship which the person whose personal information you are requesting if the Department does not already hold that information.

<sup>2</sup> If you are applying on behalf of another person other than your child or a person for whom you have legal guardianship please provide written authority and ID from that person.