

Information Privacy Policy (Institute)

This database of policies and procedures contains the current, official version of policies and associated procedures. Printing a policy or procedure or transferring a policy or procedure into another electronic format will result in the document being an uncontrolled copy that might not be current.

Purpose

The purpose of this policy is to establish a sound privacy foundation and framework in accordance with the requirements of Information Privacy Act 2000 (Vic), the Privacy Act 1988 (Cth) and the Health Records Act 2001 (Vic) and to ensure that all personal information collected, held or shared by the Institute is done so in accordance with this policy and related legislative requirements.

Scope

This policy extends to cover all operations and functions of the Institute and covers all Board members, management, employees, students, contractors, sub-contractors, vendors, service providers, customers, agents or any other third parties that have access to and/or utilise personal information collected and/or held by the Institute.

Policy

All personal and health information collected, used, held, disclosed or shared by the Institute will be in accordance with the Information Privacy Act 2000 (Vic) the Privacy Act 1988 (Cth) and the Health Records Act 2001 (Vic).

The Institute will:

- Ensure that the collection of personal information, including an individual's health information, is fair, lawful, justified and not intrusive,
- Provide access to personal information as required by the relevant legislation,
- Use or disclose personal information in accordance with the relevant legislation,
- Take reasonable steps to protect the personal information held from misuse, loss and from unauthorised access, modification or disclosure,
- Have an effective incidents/complaints handling process in place to manage privacy risks and issues and
- Ensure as a minimum that the Institute will comply with the relevant Information Privacy Principles (IPPs).

All personal information collected, held or shared by the Institute must be done so in accordance with this policy. The Institute retains the right to take reasonable steps to ensure that its Privacy Policy and Procedure are properly adhered to. Ignorance of the

existence of the Institute's Privacy Policy and Procedure will not be an acceptable excuse for non-compliance.

Definitions

"Personal Information" means information or an opinion (including information or an opinion forming part of a database) that is recorded in any form and whether true or not, about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

"Health information" is information or an opinion about the physical, mental or psychological health of an individual, a disability of an individual or an individual's expressed wishes about the future provision of health services to an individual that is also personal information and other personal information provided in connection with the donation or intended donation of the individual's body parts, organs or body substances or personal information that is genetic information which could be predictive of health.

"Sensitive information" means information or an opinion about an individual's racial/ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a trade union or association or professional association, sexual orientation or practices or criminal record that is also personal information.

Code of Conduct

All staff are expected to conduct themselves in a manner consistent with the Code of Conduct for the Victorian Public Sector and in accordance with the Box Hill Institute Code of Conduct for Staff.

Principles

These Acts are based on a number of privacy principles. The privacy principles regulate the way in which the Institute should collect, use, keep secure and disclose personal information.

The privacy principles also regulate an individual's right of access to their personal information and provide for remedies for any interference with the information privacy of an individual.

The Institute complies with the following privacy principles

1. Collection

Collection of personal information by the Institute must be fair, lawful and not intrusive.

2. Use and Disclosure

Personal or health information is only to be used or disclosed for the primary purpose for which it was collected or for one of the exceptions detailed in the Information Privacy Procedure.

3. Data Quality (Collection)

Reasonable steps must be taken to ensure that personal information collected, used or disclosed in accordance with this procedure is accurate, complete and up to date.

4. Data Security

Reasonable steps must be taken to protect the personal and health information held by the Institute from misuse and loss and from unauthorised access, modification or disclosure. All contractors engaged to dispose of Institute assets such as desktop and laptop computers and must guarantee to wipe all drives clean off existing data.

5. Openness

The Institute must set out in a document clearly expressed policies on its management of personal information. The Institute, upon the request by a person, must also take reasonable steps to let that person know generally for what purposes and how it collects, holds, uses and discloses that information.

6. Access and Correction

The Institute will provide an individual access to personal information held by the Institute. This is subject to some exceptions allowed by law. Reasons must be provided where access is denied.

7. Unique Identifiers

The Institute will not allow the assigning of a unique identifier to an individual unless the assignment of the identifier is necessary to enable the Institute to carry out any of its functions efficiently.

8. Anonymity

Where an individual elects to remain anonymous and where it is practicable and lawful to do so, the Institute will protect the anonymity of individuals in their interactions with the Institute.

9. Transborder Data Flows

Personal information to a recipient outside of Victoria (including a recipient in a foreign country) is only permitted in circumstances where the information will have the appropriate protection.

10. Sensitive Information

Sensitive information about an individual may not be collected unless:

- The individual has consented or

- The collection is required under law or
- The collection is necessary to prevent or lessen a serious or imminent threat to the life or health of an individual where the individual concerned
 - Is physically or legally incapable of giving consent to the collection or
 - Can not communicate that consent or
 - The collection is necessary for the establishment, exercise or defence of a legal or equitable claim.
- The collection is necessary for research or the compilation of statistics that is relevant to government funded targeted welfare or educational services and
- There is no reasonably practicable alternative to collecting the information for this purpose and
- It is impracticable for the Institute to seek the individual's consent to the collection.

11. Transfer or closure of the practise of a health service provider

Where a health service provided by the Institute is sold, transferred or closed down, the Institute will comply with the requirements of the Health Records Act 2001, Health Privacy Principle 10.

This principle sets out requirements for public and individual notification of the manner in which the Institute proposes to deal with the health information held by the Institute.

12. Making information available to another health service provider

Health information about an individual may not be transferred to another health service provider without the individual's consent.

Responsibility/Authority

For every Centre or Business Unit of the Institute, where personal information is collected, the **Manager** responsible for that Centre or Business Unit is responsible for the personal information collected and for ensuring compliance with this Procedure and the related Privacy Policy. In relation to students, Managers are responsible for receiving requests from employers about apprentices, supplying interim reports and locating students in an emergency.

Employees and other relevant parties are responsible for ensuring compliance with this procedure in relation to the collection, use and disclosure of personal and health information.

The Chief Financial Officer is responsible for investigating breaches, informing employees and other relevant parties that this Privacy Policy and related Procedure is established, maintained and will be enforced, periodically advising employees and other relevant parties of any changes or any new privacy policies and procedures in a timely

manner, arranging for periodical audit of compliance and responding to queries in relation to the Institute's privacy practises.

The Privacy Officer, in conjunction with the Chief Financial Officer, is responsible for investigating breaches, informing employees and other relevant parties that this Privacy Policy and related Procedure is established, maintained and will be enforced, periodically advising employees and other relevant parties of any changes or any new privacy policies and procedures in a timely manner, arranging for periodical audit of compliance and responding to queries in relation to the Institute's privacy practises.

The **Executive Director, Organisation Development** is responsible for ensuring the induction process and employment contracts reflect the Institute's information privacy obligations and procedure and overseeing any disciplinary action arising from a breach of this procedure or related legislation.

The **Registrar** is responsible for ensuring student privacy and the confidentiality of information.

In relation to student information, **Staff** are responsible for referring requests for information to the Registrar.

The **Freedom of Information Officer** is responsible for responding to FOI requests in line with the FOI Act.

The **Centre Manager, Human Resources** is responsible for responding to requests for access from staff.

The **Manager, Student Support Services** is responsible for responding to requests for access from recipient of student welfare and health services provided by the Institute through its student support unit.

The **Chief Executive Officer** is responsible for hearing appeals against Freedom of Information decisions

Records

Records will be held in compliance with the Information Privacy Act 2000 (Vic), the Privacy Act 1988 (Clth) and the Health Records Act 2001(Vic).

References and Compliance Requirements

Information Privacy Act 2000 (State)

Privacy Act 1988 (Clth)

Health Records Act 2001 (State)

Freedom of Information Act 1983 (Vic)

Freedom of Information Act 1983 (Clth)

Whistleblowers Protection Act 2001 (Vic)

Privacy Victoria, Website Guidelines for the Victorian Public Sector (May 2004) at

Related Documents

[Institute Information Privacy Procedure](#)

[Student Privacy and Confidentiality Policy and Procedure](#)

[Collection, Storage and Access to Staff Information Procedure](#)

[Student Discipline Policy and Procedure \(Institute\)](#)

[Staff Discipline Policy and Procedure \(Institute\)](#)

[Fair Treatment Procedure \(Institute\)](#)

[Whistleblowers Protection Policy and Procedure \(Institute\)](#)

[Records Management and Disposal Policy and Procedure \(Institute\)](#)

[Staff Induction Policy & Procedure](#)

Review

This procedure must be reviewed no later than five (5) years from the date of endorsement. The policy will remain in force until such time as it has been reviewed and re- approved or rescinded. The procedure may be withdrawn or amended as part of continuous improvement prior to the scheduled review date.

Further information regarding the operation of this procedure can be obtained by emailing

Privacy@bhtafe.edu.au

DOCUMENT CONTROL

Policy ID:	POLLR04
Classification:	Governance
Approved by:	The Board
Date Approved:	25 August 2005
Board Reference:	Board Meeting 06/05 25 August 2005
Committee Reference:	NA
Prepared by:	Chief Financial Officer
Accountable Manager:	Chief Financial Officer
