Privacy & Data Protection Procedure - Box Hill Institute

Related Policy	Privacy & Data Protection Policy BHI

Procedure:	Responsibility
1. In all Box Hill Institute practices staff will enact the requirements of the Information Privacy Principles (IPP) Under the *Privacy and Data Protection Act* 2014 as detailed below:	
a) **IPP 1 Collection -** Collect only personal information that is necessary for performance of functions. Advise individuals that they can gain access to personal information. Ensure persons from whom we are collecting personal information are informed: • of the primary purpose for collecting the information and to whom it would be disclosed (when, why and how); • their right to access and correct, any information; • if their information may be stored with a third party provider; and • how to directly access or request access to their personal information.	All staff collecting personal information
b) **IPP 2 Use and disclosure**-Use and disclose personal information only for the primary purpose for which it was collected or a secondary purpose the person would reasonably expect. Use for secondary purposes should have the consent of the person unless: • the secondary purpose for use and disclosure is related to the primary purpose and a person would reasonably expect such use or disclosure, and • the use or disclosure is necessary for research or the compilation or analysis of statistics in the public interest and the form it is published in does not identify any particular individual, and • there are circumstances related to public interest such as law enforcement and public or individual health and safety and welfare, or where the use or disclosure is required by or under law.	All staff with access to personal information
c) **IPP 3 Data quality**-Make sure personal information is accurate, complete and up to date. All staff will follow data collection procedures to ensure that personal information collected, used or disclosed is accurate, complete and up to date.	All staff managing personal information
d) **IPP 4 Data security**-Take reasonable steps to protect personal information from misuse, loss, unauthorised access, modification or disclosure. An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose. All staff ensure they take all reasonable steps to protect personal information from unauthorised inadvertent disclosure while: • in a shared workspace or a public place, • using personal and health information on a desk via paper or computer. If left unattended information must be made inaccessible (lock computer, lock paper away) to unauthorised persons,	All staff with access to personal information

• emailing or faxing , • using portable storage devices outside the workplace (information contained should be encrypted and have secure protection such as password-protected access. Lost smart phones should be immediately disabled remotely. BHI will establish and promote responsible data security regime and practices to staff and students.	
e) **IPP 5 Openness**-Document clearly expressed policies on management of personal information and provide the policies to anyone who asks. Policy and procedure are available on BHI staff intranet and Privacy and personal information statements are published on the Institute websites.	Nominated staff
f) **IPP 6 Access and correction**-Individuals have a right to seek access to their personal information and make corrections. Access may also be managed under the *Victorian Freedom of Information Act 1982.* Unless a legal exemption exists the Institute will correct information where a written request is received by the following staff: • For staff information-Operations Manager, Business Partner; • For students information-the Registrar ;and • For students information relating to health (disability or welfare), Manager Student Support Services.	All staff collecting and managing personal information
Exemptions from providing access to or correcting information include: • documents covered by the *Freedom of Information Act 1982* (refer to Freedom of Information Procedure, or seek advice from the General Counsel & Company Secretary General Counsel and Company Secretary); • where providing access would pose a serious and imminent threat to the life or health of any individual; • providing access would have an unreasonable impact on the privacy of other individuals , and • providing access would be unlawful or prejudice, or be likely to prejudice an investigation into unlawful activity.	All staff collecting personal information
g) **IPP 7 Unique identifiers**-A unique identifier is usually a number assigned to an individual in order to identify the person for the purposes of an organisation's operations. Tax File Numbers and Driver's Licence Numbers are examples. Unique identifiers can facilitate data matching. Data matching can diminish privacy. BHI staff will limit the adoption and sharing of unique identifiers by: • only assigning a unique identifier when required for an identifiable and required function, and • only using a unique identifier that was generated by a non-Institute entity, (unless they have the written consent of the person involved) if required to meet an Institute function, including performance of a contract with a State or Commonwealth Department.	Student administration and People and Culture, registrar
h) **IPP 8 Anonymity**-Give individuals the option of not identifying themselves when entering transactions with organisations, if that would be lawful and feasible. • If practical and lawful the Institute will offer the option of the person	All staff

not being identified in any transaction.	

i) **IPP 9 Trans border data flows**- when personal information travels, privacy protection should travel with it. Transfer of personal information outside Victoria is restricted. Personal information may be transferred only if the recipient entity protects privacy under *enforceable* standards similar or equal to Victoria's Information Privacy principles.
• Before any transfer of personal information outside of Victoria the Institute will ensure the information about the person involved will be given similar level of protection and the person is asked for consent to the transfer;
  • If obtaining consent is not practical, the transfer is necessary for the performance of a contract or delivery of services to the person, and is in the interests of the person involved ,and
  • That a reasonable view can be formed that if the person could consent they would likely do so.
	All staff dealing with personal information in this context

j) **IPP 10 Sensitive information**-The law restricts the collection of sensitive information like an individual's racial or ethnic origin, political views, religious beliefs, sexual preferences, membership of professional or industrial groups or criminal record. Sensitive information will only be collected if it fits a specific category of use as outlined by the *Privacy and Data Protection Act 2014.* These include: • Where the person consents, • Where it is required by law, • Where 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 cannot communicate that consent, or the collection is necessary in relation to a legal or equitable claim, • Where there is government funded research and no other means of information collection is practicable to obtain that information, *and* where obtaining consent is not practical. Advice should be sought from the Institute's General Counsel & Company Secretary before relying on these exemptions.	All staff dealing with personal information in this context
2. Dealing with Health Information (Health Records Act 2001) a) Where a health provider that the Institute owns is sold, transferred or closed down the Institute will comply with Health Records Act "Health Privacy Principle 104" b) Where a person requests transfer of their own health information (see definition in policy) to another health provider this request must be in writing (with appropriate verifiable identification): • *For staff*-to the Executive Director, Corporate Services using the *Application to Access Personal or Health Information* form, • *For BHI students*-to the Registrar (where information is about use of Institute's welfare or disability services, to the Manager Student Support Services)	Nominated staff
3. Enacting all other privacy related requirements a) **Use of images taken by Institute**: All persons prominent in any image (photo, video) taken by and used by the Institute must sign a consent form for use of that image. The consent	All staff

form must be kept as long as the image is used. Where consent is not practical, at any event where the Institute is capturing images, prominent signs must be posted to alert attendees that images are being taken for Institute use. **b) Personal Information & Data Privacy Collection Notices** Individual privacy notices will be published on relevant documents outlining privacy protection requirements, including electronic documents when they are made available to users. c) **Contractual requirements**-(the role of contractors in privacy) When outsourcing Institute functions, third party contractors must also be bound by the Victorian Information Privacy principles).To ensure this, a clear, *Information Privacy Contract Clause(s*) must be included. d) **Information classification by Institute**. All Institute data and personal information will be classified and secured according to its level of sensitivity and in compliance with the *Victorian Protective Data Security Standards* and the protective data security regime of BHI.	All staff designing forms and notices Staff involved in preparing contracts All staff
4. Disciplinary actions relating to non-compliance with Privacy & Data Protection Policy or Procedure a) BHI will provide a consistent and fair procedure for handling complaints with respect to privacy of personal information. This procedure will apply if an individual considers that the Institute has acted in a manner that breached a Privacy Principle in respect of that individual. b) Staff has a duty to take all reasonable steps to meet the requirements of the Privacy & Data Protection Policy and this Procedure. c) In addition staff and third party contractors (who are also bound by this requirement) must notify the General Counsel & Company Secretary if they learn of or reasonably suspect a privacy breach has occurred during Institute operations. d) Complaints can be directed to the BHI Privacy Officer contact: privacy@boxhill.edu.au, or in writing to: Privacy Officer General Counsel & Company Secretary Box Hill Institute, Elgar Campus, 465 Elgar Road Box Hill 3128 Victoria e) Alternatively a person may contact the Privacy and Data Protection Commissioner at: Commissioner for Privacy and Data Protection PO Box 24014 Melbourne Victoria 3001 Phone: 1300 666 444 Email:privacy@cpdp.vic.gov.au **Making and managing a complaint** f) A written complaint must be forwarded to the General Counsel & Company Secretary within six months of the time the complainant first became aware of the alleged breach. The complaint must specify details of the alleged breach. g) The General Counsel & Company Secretary must make a determination on the complaint within 45 days of receipt of the complaint, and advise the	All staff

complainant in writing. h) If the General Counsel & Company Secretary determines that there has been a breach of the Privacy Principles, he or she will, upon notification of the determination to the complainant, advise relevant Institute personnel in writing of any action required in order to remedy the breach. If the breach is capable of being rectified and is not rectified within (30) days of the advice from the General Counsel & Company Secretary, the General Counsel & Company Secretary must inform the CEO. i) The General Counsel & Company Secretary will keep a record of all complaints. This will comprise a register and file records that will be securely stored in accordance with the *Privacy and Data Protection Act 2014 (Vic).* **Consequences if the Privacy Policy is breached:** j) Staff who fail to take reasonable steps to meet the requirements of the policy or procedure may be subject to disciplinary action under the Institutes Disciplinary Policy and Procedure.	

5. Incident Management
A data breach is when personal information held by BHI is lost or subjected to unauthorised access, modification, disclosure, or other misue orinterference. For example, when a device containing personal information is lost or stolen, a database containing personal information is hacked or personal information is mistakenly provided to the wrong person.
a) Incident Response Plan
• Contain the breach
  ○ Do what you can to stop the suspected breach (e.g. stop the practice, recover the records, shut down the system that was breached)
• Evaluate the risks
  ○ Record and advise of the time and date the suspected breach was discovered, the type of personal information involved, the cause and extent of the breach, and the content of the affected information and the breach
  ○ Ensure evidence is preserved that may be valuable in determining the cause of the breach
  ○ Assess priorities and risks based on what is known
  ○ Keep appropriate records of the suspected breach and actions in response, including the steps taken to rectify the situation and the decisions made
• Notification
  ○ Staff to immediately notify their Director/Manager of the suspected breach
  ○ Alert the Privacy Officer/Legal team regarding the suspected breach
  ○ Determine who needs to be made aware of the breach (internally and potentially externally)
  ○ Determine whether to notify affected individuals – is there a real risk of serious harm to the affected individuals?
  ○ Consider whether others should be notified, including police or other agencies or organisations affected by the breach.
• Prevent future breaches
  ○ Fully investigate the breach
  ○ Make appropriate changes to policies and procedures if necessary
  ○ Revise staff training practices if necessary
  ○ Update security and response plan if necessary
b) Incident Register
• Records of all incidents will be stored on the Incident Register, managed by the General Counsel & Company Secretary
	All Staff

• The Incident Register will record date the suspected breach was discovered, the type of personal information involved, the cause and extent of the breach, and the content of the affected information and the breach, details of the investiation by BHI and any response and follow up.	
6. Student Privacy *Note that this section is subject to the requirements of section two of this Procedure:* ***Dealing with Health Information (Health Records Act 2001).*** *Where there is a contradiction, the section two requirements prevail*. **a) Student access to their own personal information** • Students may access their own personal information (including health information) held by BHI by applying directly to the Registrar. It is not necessary for a student to make application under the Freedom of Information Act. • However, if a student is not satisfied with the information access provided, the request may be made as a Freedom of Information request. In this instance, refer to Freedom of Information Policy and Procedure.	Students
b) Student consent to release personal information about themselves Students are required to view and agree to the terms of BHI **Personal Information & Data Privacy Collection Notice** upon enrolment. By doing so students are acknowledging that their personal information may be used in accordance with that notice.	Students
c) Release of student exam and assessment results Results will only be released by Student administration by official act of the Registrar. No other staff shall release unofficial or official results.	
d) Students wanting to obtain extra copies of official results must: • Lodge in person a written request with Student Administration, and provide identification. Any fee applied must be paid when lodging request. • The request may take up to five working days to complete and can be posted or collected during working hours.	Students
e) **Releasing student information to employees** (including interim information) • If an employee, trainee or apprentice requires information in addition to the annual attendance/results information provided by the Institute, Operations Managers may on receipt of a request, and after seeking permission of the Registrar,check the Institutes official records and notify by mail or telephone the employer of the information required. The Registrar will determine the form of that notification.	Teaching Centre staff
f) **Releasing student information to Federal Police and government departments empowered to serve a notice requiring disclosure**: • Such notices will be received in writing by the Registrar, • The Registrar will ensure the right claimed is valid, • Obtain, confirm the accuracy of, and send the information to the relevant body.	Registrar Management
g) **Releasing information in compliance with a subpoena is the same process as a Federal Police request**, Registrar/Team Leader, Information Systems Management noting any delivery requirements.	
h) Request to release students information to other persons including requests from research or survey entities: • All such requests must be processed by the Registrar who will make their decision based on the Privacy Policy.	

i) Contacting students in an emergency (including requests by police): • Staff should refer to the Registrar on all campuses. • The Registrar will then contact a student counsellor who will contact the student to determine whether the student wants to meet with the person requesting contact. **j) BHI may transmit personal information or data outside Victoria if it is lawful under the Act** (e.g. only to legitimate recipients, after appropriate risk assessment of privacy protections, and when equivalent safeguards are accorded to the information/data by the recipient).	Registrar
7. Collection, access to and storage of employee information *Note: this section should be read in conjunction with section two of this Procedure and any other section that has specific requirements for dealing with information. If a contradiction is evident, advice should be sought from the General Counsel & Company Secretary.* a) **Collection and storage** is carried out by Corporate Services in compliance with their work practice, which will meet the requirements of and the policy and this procedure. b) For employees to **access their information** they must submit a request in writing to Corporate Services Business Partner if they wish to access personal or health information that relates to them, or nominate a representative to have that access refer to section two of this procedure for additional requirements for health information. c) If employees then wish to **correct information**, they should make a written application outlining the matter to their Corporate Services Business Partner. d) On receipt of a request to alter information, their Corporate Services Business Partner will register the request, make a decision and provide a written response to the requesting employee within 45 days. e) Any **request for employee information from an external authority** must be forwarded to the General Counsel & Company Secretary, who will ensure the external authority, has the legal right to receive the information. On providing the information they should also notify the relevant employee unless this is expressly forbidden by law (see sections two and six of this procedure).	Relevant Corporate Services staff member All staff

Approval Body	Chief Executive Officer
Document ID	PROLR04
Date Approved	16 December 2016
Amendment	Minor Administrative changes to remove reference to 'BHIG' and 'CAE' made by Academic Quality Assurance Officer on 8 April 2019
Owner	General Counsel & Company Secretary
Author	General Counsel & Company Secretary