UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

Policy

PROTECTION OF PRIVACY POLICY

Number: GV 2
Classification: Governance
Approving Authority: Board of Governors
Designated Executive Officer: President
Effective Date: March 2022
Supersedes: November 2018
Date of Last Review/Revision: February 2022
Mandated Review Date: February 2029

Associated Procedures: [This section will be updated as Procedures are developed and approved appropriately by the Procedural Authority].

Table of Contents

1.0 BACKGROUND 3
2.0 PURPOSE 3
3.0 SCOPE 3
4.0 DEFINITIONS 3
5.0 POLICY 5
5.1 Accountability for Personal Information 5
5.2 General 6
5.3 Collection of Personal Information 7
5.4 Consent for Collection of Personal Information 7
5.5 Use, Disclosure and Retention of Personal Information 7
5.6 Use of Surveillance Systems 8
5.7 Accuracy and Correction of Personal Information 10
5.8 Protection of Personal Information 10
5.9 Authorization to Act on Behalf 10
5.10 Storage of Personal Information 11

5.11 Retention and Disposal of Personal Information 11
5.12 Individual Access to Personal Information 11
5.13 Unauthorized Access or Disclosure of Personal Information 12
6.0 AUTHORITIES AND OFFICERS 12
7.0 RELEVANT LEGISLATION AND STANDARDS 12
8.0 RELATED POLICIES AND OTHER ASSOCIATED DOCUMENTS 13

1.0 BACKGROUND

The University has a legal and ethical obligation to protect the privacy of individuals whose information it manages. British Columbia's *Freedom of Information and Protection of Privacy Act* (FOIPPA), and the best practices outlined in the Canadian Standards Organization Model Code for the Protection of Personal Information (the Model Code), and various standards and guidelines issued by the Office of the Information and Privacy Commissioner of British Columbia inform the substance of this policy.

2.0 PURPOSE

The purpose of this policy is to establish how the University complies with the protection of privacy requirements under FOIPPA and manages Personal Information in accordance with best practices.

3.0 SCOPE

3.1 This policy applies to all personal information in the custody or under the control of the University and to all University Employees, Officers of the University, Volunteers, and Service Providers who have access to personal information.

3.2 This policy does not apply to the research information of faculty or other individuals carrying out research at the University.

4.0 DEFINITIONS

4.1 **Act or FOIPPA** means the British *Columbia Freedom of Information and Protection of Privacy Act*.

4.2 **Administrator** means an individual engaged in directing and overseeing a distinct program, unit, office, or department of the University (e.g., manager, director, dean, etc.).

4.3 **Business Contact Information** means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email, or business fax number of the individual.

4.4 **Custody of a record** means UNBC has the possession of a record and responsibility for its care.

4.5 **Control of a record** is having the authority to manage records related to a mandate or function that is relied upon for businesses purposes.

4.6 **Compelling Circumstances** are situations when someone is compelled to act to protect an individual whose health or safety is in imminent danger.

4.7 **Consent** means voluntary agreement by a person in the possession and exercise of sufficient mental capacity to make an intelligent choice to do something proposed by another; it supposes a physical power to act, a moral power of acting and a serious, determined and free use of these powers.

4.8 **Determining Custody or Control** is defined in the attached Standards (see Appendix 1)

4.9 **Disclosure** means to transmit, reveal, show, expose, provide copies of or give Personal Information or records.

4.10 **Emergency** means a present or imminent event of a short duration that affects or threatens the health, safety or welfare of people, or University property and infrastructure.

4.11 **Employee** means a person who is employed by the University and is remunerated for their work. For the purposes of this Policy and the associated procedures, each reference herein to Employee also includes Officers of the University (E.g. members of Senate and the Board of Governors), volunteers, and service providers to the extent appropriate in the context.

4.12 **Personal Information** means recorded information about an identifiable individual other than business contact information.

4.13 **Personal Information Bank (PIB)** means a collection of personal information that is organized and capable of being retrieved using an individual's name or an identifying number or some other personal identifier.

4.14 **Privacy Breach** means access to or collection, storage, retention, disposal, use or disclosure of personal information that is not authorized by the *Act*.

4.15 **Privacy Impact Assessment (PIA)** means a compliance and risk-based assessment conducted by the University to determine if a current or proposed system, project, program, or activity meets or will meet the protection of privacy requirements of the Act. It is a risk management and compliance tool used to identify and correct or mitigate potential privacy and security issues, thus avoiding

Privacy Breaches, harm to institutional reputation or costly program, process or service redesign. Conducting Privacy Impact Assessments is a legal requirement under FOIPPA.

4.16 **Service Provider** means a person or company retained under contract to perform services for the University.

4.17 **Surveillance System** means overt and covert cameras recording both audio and/or visual images to monitor behavior, activities, or information

4.18 **University** means the University of Northern British Columbia (UNBC).

4.19 **University Community** means all students and employees of the University and all people who have a status at the University mandated by legislation or other University policies, including research assistants, post-doctoral fellows, Officers of the University including members of Senate and the Board of Governors, volunteers, visiting faculty, emeritus faculty, and visiting researchers.

4.20 **Volunteer** means a person who does work for the University without being paid.

5.0 POLICY

5.1 Accountability for Personal Information

5.1.1 Through this Policy, the Board of Governors designates the President as the head of the public body under the *Act*.

5.1.2 In accordance with section 66 of the *Act*, the President may delegate the duties of Privacy Officer to an employee or employees through a formal written document. A memo outlining any such delegation must be copied to the Chair of the Board of Governors, and maintained in the records of the Board of Governors.

5.1.3 The Governance Officer – Access, Privacy and Records Management is responsible for promoting, monitoring, and reporting on compliance with the FOIPPA and with University access, privacy, and records management policies. The Governance Officer's responsibilities include the following:

i. providing privacy advice and training;
ii. providing ongoing assessment of privacy risks;
iii. responding to privacy complaints and investigating concerns about privacy issues; and

iv. investigating and/or recommending to the appropriate administrative authority corrective action, suspension, or termination of a project or activity where the Governance Officer establishes that there is a significant privacy risk.

5.1.4 Administrators are responsible for the following:

i. making reasonable efforts to familiarize themselves with the requirements in the FOIPPA, this policy and its associated procedures, and for making reasonable efforts to communicate these requirements to the Employees in their Units;
ii. making reasonable efforts to ensure that the management of Personal Information in the custody or under the control of their units meets the requirements of the FOIPPA, this policy and its associated procedures;
iii. reporting any privacy incidents or breaches of FOIPPA, this policy or its associated procedures in accordance with the University's Procedures for Responding to a Privacy Incident or Breach; and
v. conducting privacy impact assessments.

5.1.5 All Employees who collect, access, use, disclose, maintain and dispose of Personal Information are in a position of trust. Employees are responsible for the following:

i. treating all Personal Information to which they receive access in accordance with the FOIPPA and this policy;
ii. making reasonable efforts to familiarize themselves and to comply with the requirements in the FOIPPA, this policy, and its associated procedures;
iii. consulting as necessary with the appropriate authority regarding the requirements in the FOIPPA, this policy, and its associated procedures; and
iv. reporting any privacy incidents or breaches under the FOIPPA, this policy, or its associated procedures.

5.1.6 The University requires a third party service provider whose work on behalf of the University involves the collection, use or Disclosure of Personal Information to abide by this policy, the Privacy Protection Schedule, and FOIPPA in its handling of personal information on behalf of the University. The University may require the service provider to sign a confidentiality agreement.

5.2 General

5.2.1 All personal information must be managed by the University in compliance with *the Act* as specified below and in accordance with best practices and standards for the protection of personal information.

5.2.2 The collection, access, use, disclosure, and retention of personal information must be limited to information that is directly related to and necessary for University operations.

5.2.3 Every reasonable effort must be made by the University to ensure the accuracy and protection of personal information in its custody or control.

5.3 Collection of Personal Information

5.3.1 Personal information must be collected only as provided for under Part 3 of the *Act*, and appropriate notice and methods of collection are used at all times.

5.3.2 The collection of personal information must be limited to the minimum amount necessary to carry out the University's activities as mandated by the *University Act*.

5.4 Consent for Collection of Personal Information

The University normally obtains express or implied consent from an individual before collecting Personal Information, but may collect, use or disclose Personal Information without consent in limited circumstances as authorized by FOIPPA.

5.5 Use, Disclosure and Retention of Personal Information

5.5.1 Employees are only granted access to personal information necessary for the performance of their duties.

5.5.2 Personal information is only used
- i. for the purpose in which it was obtained or compiled or for a use consistent with that purpose;
- ii. with the written consent of the individual who the personal information is about;
- iv. for the purpose it was disclosed to the University; or
- v. for any other purpose permitted under the *Act*.

5.5.3 The University must not disclose any personal information of students, employees, alumni, retirees, clients, and donors in its custody or under its control to any third party, unless doing so is provided for under the *Act*.

5.5.4 Disclosure of the following information without consent is permitted:
- i. an Employee's contact information;
- ii. information about an individual's position, functions, or remuneration as an officer, Employee, or member of the University;

iii. names of individuals who have received degrees, the names of degrees those individuals received and the years in which the degrees were awarded;
iv. Personal Information about an individual in an emergency situation or where the Director, Safety and Security determines that compelling circumstances exist that affect anyone's health or safety, or as permitted by the associated *Disclosure of Student Information in Emergency or Compelling Circumstances Procedures*.

5.6 Use of Surveillance Systems

5.6.1 It is lawful for the University to collect personal information only in circumstances permitted by s. 26 of FOIPPA. The University must be prepared to demonstrate to the public and to the OIPC, with specific evidence, that one or more provisions of s. 26 of FOIPPA authorize its proposed or existing collection of personal information by a surveillance system.

5.6.2 Each component of the surveillance system, be it overt or covert, must be lawful. For example, when UNBC is considering implementing or enhancing an already existing surveillance system that collects video and audio footage, it should be able to demonstrate the purpose and the legal authority for both. All requests for authorization must include evidence that supports how each component fulfils the purpose of the collection.

5.6.3 UNBC may use Surveillance Systems to:
i. improve personal safety on University property by acting as a deterrent or increasing the likelihood of identifying individuals who may commit criminal activity;
ii. assist law enforcement agencies with the investigation of any suspected criminal activity;
iii. assist with the protection of University assets and infrastructure; or
iv. assist with the application of University policies.

5.6.4 Surveillance Systems must not be used to monitor or record areas where the University Community or public have a reasonable expectation of privacy.

5.6.5 Surveillance Systems must only be deployed as an exceptional step to address real, pressing, and substantial problems or risks and only where a less privacy-invasive alternative is not available.

5.6.6 Surveillance Systems must be designed to minimize the impact on privacy. The privacy impact of the proposed Surveillance System needs to be

assessed and documented in the PIA prior to installation, upgrade, enhancement or replacement of the system.

5.6.7 Approval is required prior to installation, upgrade or enhancement of a Surveillance System. The Director, Safety and Risk is responsible for approval of the installation and all requests must provide written confirmation that the installation is necessary to address real, pressing and substantial problems or risks and that a less privacy-invasive alternative is not available.

5.6.8 The Director, Safety and Security must have the approval of installation confirmed with the Governance Officer – Access, Privacy and Records Management, in relation to privacy considerations, and the Vice President, Finance and Administration before finalizing the approval.

5.6.9 A written request for use must be sent to the Director, Safety and Risk that outlines the following:

i. the requestor's name, department and position;
ii. the rationale for use of surveillance;
iii. the less intrusive methods considered and why they were rejected;
iv. who is authorized to view and share the personal information recorded; and
v. how the information will be stored, for how long and when it can be expected to be deleted.

5.6.10 Section 32 of FOIPPA limits the purpose for which a public body can use personal information. UNBC should be prepared to demonstrate it is using personal information properly and is meeting the requirements of section 32.

5.6.11 Information collected through video or audio surveillance should not be used beyond the original purpose for the collection and any other purpose that is demonstrably consistent with this purpose.

5.6.12 Surveillance systems are collecting Personal Information whenever they are recording regardless of if, or how, UNBC uses, retains or discloses the recordings in the future.

5.6.13 The Director, Safety and Security is responsible for keeping a list of all covert and overt cameras, their location and their capabilities (including, but not limited to, video and audio recording abilities, web-enabled, cloud-based system and take special note if any surveillance records are available or can be viewed by any party external to UNBC such as vendors, law enforcement or staff working in remote or isolated environments). This list must be shared with the Office of University Governance annually.

5.6.14 If the installation of a surveillance system is for a time-limited specific investigation into criminal conduct, it must be approved by the Vice President, Finance and Administration. Covert surveillances must only be approved if they are essential to the investigation, and the need for them outweighs the privacy issues of those that could be observed. Covert surveillance must not be authorized on an ongoing basis.

5.6.15 The University must provide notice of the use of overt surveillance systems by prominently displaying signage at the perimeter or entrance to the area being monitored or recorded to alert individuals that such systems are or may be in use before they enter any area under surveillance

5.7 Accuracy and Correction of Personal Information

5.7.1 The University must make every reasonable effort to ensure the personal information it uses to make decisions that directly affect individuals is accurate and complete.

5.7.2 Upon request by an individual to whom the personal information relates, the University corrects, makes additions to, or annotates the information with a correction when documentary evidence, satisfactory to the University, is provided to substantiate the correction.

5.8 Protection of Personal Information

5.8.1 The University protects personal information by making reasonable policy, procedural, physical, and technical security arrangements against such risks as unauthorized access, collection, use, disclosure, or disposal.

5.8.2 The University ensures that the protection of personal information is a core consideration in planning, implementing and maintaining new and revising existing systems, projects, programs or activities by completing Privacy Impact Assessments.

5.9 Authorization to Act on Behalf

5.9.1 If someone is requesting personal information about another individual, they are required to have an Authorization to Release Statement signed by that individual and submitted as part of the request. Under FOIPPA, there are very few specific exemptions in which personal information can be provided to a third-party without their consent.

5.9.2 Third party individuals or organizations (E.g. parents, agents, employers, sponsors etc.) must be authorized by the individual (in writing) in order for UNBC to release any information.

5.9.3 *Authorizations to Release Statements* are normally only valid for one year from date signed.

5.9.4 In most cases, authorizations are only for a specific item or two, and not a blanket approval to do everything with them. This must be respected.

5.9.5 Privacy breaches must be managed by the University in an effective and timely manner, in accordance with the *Privacy Breach Procedures*.

5.10 Storage of Personal Information

5.10.1 The University prefers to store all personal information in its custody or control only inside Canada, unless the individual the information is about has consented to storage outside Canada or unless the storage is permitted under the *Act*.

5.10.2 A PIA must be conducted

i. for new initiatives where a PIA was not formerly conducted;
ii. before implementing a significant change to an existing initiative; or
iii. when personal information is stored, accessed or disclosed outside of Canada;

5.11 Retention and Disposal of Personal Information

5.11.1 The University retains an individual's personal information for at least one year when it is used to make a decision that directly affects the individual.

5.11.2 Unless section 5.11.1 is applicable, video files are erased within one month unless retained at the written request of the Director, Safety and Security or if needed to document an ongoing incident or investigation.

5.11.3 The disposal of personal information is done securely and the destruction of the information is documented accordingly.

5.12 Individual Access to Personal Information

5.12.1 Individuals have a right to access Personal Information about themselves, subject to exceptions under the FOIPPA. FOIPPA does not replace other

procedures for access to information or limit in any way access to information that is not personal information and is available to the public.

5.12.2 Individuals have a right to request corrections to Personal Information about themselves, subject to exceptions under the FOIPPA

5.13 Unauthorized Access or Disclosure of Personal Information

5.13.1 It is an offence under FOIPPA to disclose personal information in contravention of the *Act*.

5.13.2 Any employee of the University who is aware of an unauthorized disclosure of personal information, or who suspects there has been an unauthorized disclosure of personal information, must immediately notify the Office of University Governance's Access, Privacy and Records Management Governance Officer (Privacy Officer).

5.13.3 All privacy complaints related to this Policy or under the *Act* must be made in writing to the Office of University Governance and be addressed to the Governance Officer – Access, Privacy and Records Management.

5.13.4 The University responds to all complaints about breaches of privacy in accordance with the *Act* and discloses the outcome of any investigation to the complainant as per the *Privacy Breach Procedures*.

6.0 AUTHORITIES AND OFFICERS

The authorities and officers for this policy are as follows:
Approving Authority: Board of Governors
Designated Executive Officer: President
Procedural Authority: President
Procedural Officer: Senior Governance Officer

7.0 RELEVANT LEGISLATION AND STANDARDS

- *University Act*, R.S.B.C. 1996, c. 468
- *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165
- *Canadian Anti-Spam Legislation*, S.C. 2010, c. 23
- Canadian Standards Organization Model Code for the Protection of Personal Information [CAN/CAS-Q830-96]
- Office of the Information and Privacy Commissioner of British Columbia's guideline on "Privacy Breaches: Tools and Resources" (March 2012)
- International Standards Organization Guidelines (ISO 29134 Guidelines)

8.0 RELATED POLICIES AND OTHER ASSOCIATED DOCUMENTS

8.1 Appendix 1 Determining Custody and Control Standards

8.2 Appendix 2 Protection of Privacy – Defining Personal Information