UNIVERSITY OF NORTHERN BRITISH COLUMBIA

Employee Privacy Handbook

Privacy and Access team
Direct Line: 250-960-5850

Email: privacy@unbc.ca

Office of University Governance
2023 CJMH
3333 University Way
Prince George, BC Canada V2N 4Z9

INDEX

UNBC Privacy Overview

Introduction

In our daily interactions with staff, students, and others, handling personal information is key. UNBC values safeguarding this information not just as a rule but as a core part of our commitment to trust and responsibility. This Privacy Handbook guides staff in adhering to set standards, fostering a culture of privacy awareness at UNBC.

Our Privacy Responsibilities

UNBC follows the BC's Freedom of Information and Protection of Privacy Act (FOIPPA), which is a law that regulates personal information practices. Compliance with FOIPPA is mandatory for all UNBC employees. Additionally, UNBC complies with the Canadian Anti-Spam Legislation (CASL) to ensure that external electronic communications that are commercial in nature align to legal standards.

Accountability for Personal Information

The Office of University Governance, oversees UNBC's privacy compliance and our privacy activities are led by the Privacy and Access team. Our Protection of Privacy Policy emphasizes that employees handling personal information hold positions of trust. All employees are responsible for treating personal information in line with FOIPPA and the Protection of Privacy Policy requirements.

1. What is Personal Information?

Personal information is defined under FOIPPA as **"any recorded information about an identifiable individual"**. It includes information that can be used to identify an individual through association or inference.

Exception: Business contact information is not personal information (i.e., information about your job such as your UNBC email, office location, position title, etc.).

Examples of Personal Information Include:

- ***Profile**: Name, Age, Sex, Height, Weight*
- *Home Phone Number*
- *Home Address*
- *Medical History*
- ***Biometric**: Fingerprints, facial features*

What Personal Information is "Sensitive"?

Some types of personal information can be considered sensitive because there is a significant risk of harm to individuals if the information is improperly collected, used, or disclosed.

The term "significant harm" includes a range of serious negative outcomes such as identity theft, substantial physical injury, embarrassment, harm to one's reputation or relationships, loss of job, business, or professional prospects, financial loss, adverse effects on credit history, and the damage or loss of property.

Determining sensitivity depends on factors such as the nature of the data, the context, and the potential consequences for individuals.

A student's date of birth may sometimes be publicly available, however, where the person has concerns about identity theft, it may be sensitive.

2. Staff Responsibility for Protecting Personal Information

a) Collection of Personal Information

FOIPPA establishes that UNBC can directly collect personal information for activities essential to university operations. As a UNBC staff or faculty member, it is your responsibility to ensure you follow the appropriate processes for collecting personal information from individuals.

Some tips for properly collecting personal information include:

I. Direct vs. Indirect Collection

Direct Collection: Personal information should be collected directly from an individual unless exceptions exist.

Example: Kelly, a student, registers to attend a UNBC event and provides her name, email, and dietary restrictions. This information is directly given by Kelly and is permitted.

Indirect Collection: Indirect collection of personal information is not permitted except if it falls under an exception provided by FOIPPA.

FOIPPA exceptions for indirect collection include where it is a) Permitted by the individual, b) Permitted by law, c) Necessary for medical treatment and cannot be collected directly, d) Needed for awards, e) Legal proceedings, f) Debt collection, or g) By law enforcement.

II. Collection of Personal Information Must be Necessary

What can be considered unnecessary?

- Collecting personal information without a defined need, such as collecting a student's date of birth on a form without a specific purpose.
- Collecting personal information indiscriminately, for example, using multiple forms to gather similar information.
- Collecting personal information "just in case".

Ensure that you identify and document the **purpose** for obtaining personal information.

III. Provide a Collection Notice

Individuals must be informed about the personal information collected from them; we do this by providing collection notices at various points of personal information collection. This notice must include:

- The purpose for collecting their personal information.
- The legal authority under FOIPPA for collecting their personal information.
- Contact information for a UNBC employee they can reach out to for questions or issues.

b) Use of Personal Information

UNBC employees are only granted access to personal information necessary for the performance of their duties.

UNBC's Protection of Privacy Policy states that personal information must only be used for the purpose it was obtained, or for a use consistent with that purpose.

Purpose for which personal information was obtained:

- This means that personal information collected from individuals should only be used for the specific reason it was collected.

Example: If we collect a student's contact details for administrative purposes, it should not be used or shared to a third-party for marketing purposes.

Consistent use:

- The use of personal information should align with the original reason it was collected. Even if not the exact same purpose, it should be a reasonable and closely related use.

Example: If we collect personal information for organizing an event, we may use it to send relevant updates about the event or to ask for feedback after such event.

c) Disclosure of Personal Information

Employees must keep personal information that they manage or have access to confidential and should not share it with any third parties. However, there are exceptions to this rule as outlined by FOIPPA.

Examples of situations where disclosing information is considered acceptable include:

- Providing an employee's work-related contact information.
- Revealing details about an employee's job responsibilities, duties, or salary.
- Disclosing names of individuals who have received degrees, the type of degrees they were awarded, and the years these degrees were conferred.
- In urgent scenarios where there is a threat to health or safety, or in other cases specified by the University's procedures for emergency information disclosure.

d) Retention of Personal Information

Every UNBC employee manages the records they create or receive. The University's Protection of Privacy Policy mandates retaining personal information used to make decisions for at least one year after its use. Employees must avoid retaining records permanently.

Seek guidance from the Privacy and Access team when retention periods are undefined.

e) Storage of Personal Information

UNBC prioritizes storing personal information within Canada. Employees must notify the Privacy and Access team via email at privacy@unbc.ca if proposed systems may store information outside Canada. Only approved internal systems must be used for storage. The duplication of personal information is discouraged.

Example: Information received through email may be stored in various locations, including email folders, SharePoint sites, and locally on a desktop. If this information is subsequently stored on an approved system, ensure that it is deleted from all other systems where it was previously stored, including email.

3. Privacy Rights

a) What Privacy Rights do Individuals Have?

If UNBC holds personal information about an individual, that person has specific rights concerning their data.

These rights include:

Right of Access

Individuals can inquire with UNBC about the personal information held about them.

Right to Request Correction

Individuals can contact UNBC to correct inaccurate personal information or provide missing details.

b) Handling Access Requests

Requests by an individual to exercise their privacy rights may be directed to you as an employee or to your department. Once you receive such a request, UNBC has 30 days to fulfill it. It is your duty to promptly forward these requests to privacy@unbc.ca so that the Privacy and Access team can guide the response to the request.

In specific cases, the requested record may be under the control of an employee, and the Privacy and Access team may seek your support to fulfill the request. This could involve providing the requested record or making necessary corrections.

In certain cases, we may be unable to process a request due to legal constraints. Its important to forward all requests to the Privacy and Access team to provide guidance on which requests we can legally fulfill and which we cannot

4. Privacy Breaches

a) What is a Privacy Breach?

A privacy breach occurs when unauthorized (illegal or accidental) access, collection, use, or disclosure of personal information takes place.

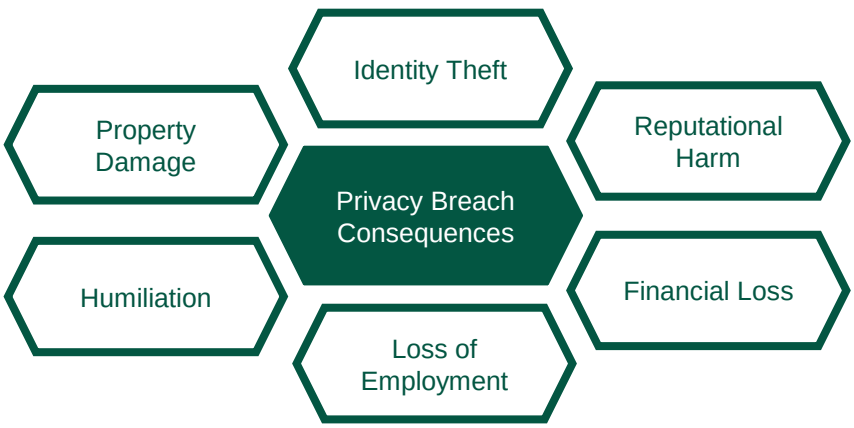
Privacy breaches occur more frequently than we think; a common example is sending an email that contains personal information to the wrong recipient.

Examples of privacy breaches include:

- Unintentional posting of student grades on a public bulletin board
- Printing documents containing social insurance numbers and leaving them unattended
- Uploading student disciplinary records to an unsecured cloud platform
- Leaving a laptop with access to student profiles unlocked and unattended
- Disposing of paper documents with personal information, such as student addresses and contacts details, into public waste bins

b) Consequences of Privacy Breaches

Privacy Breaches have consequences for both UNBC and individuals who are affected.



c) Handling a Privacy Breach

It is your responsibility to promptly report any suspected privacy breach incidents to your supervisor and the Privacy and Access team via email at privacy@unbc.ca. If the activity constituting the breach is ongoing, you must immediately cease the activity. The Privacy and Access team may require your assistance in responding to the breach, and it is your duty to provide support.

5. Privacy Impact Assessments (PIAs) at UNBC

a) What is a PIA?

A PIA serves as a proactive risk-management and compliance tool within UNBC. We use PIAs to identify and manage potential privacy issues associated with the collection, use, and disclosure of personal information.

b) When is a PIA Required?

PIAs are necessary whenever UNBC is introducing a new program, system, service, or is making modifications to an existing one that entails the collection, use, or disclosure of personal information.

Examples of situations where a PIA is needed include:

- Making changes to the strategies for engaging with alumni, including updates to alumni databases or communication platforms.
- A department is considering outsourcing certain student services to a third-party service provider.
- UNBC implements updates or modifications to its Learning Management System that involve additional data fields and functionalities.
- A faculty member introduces a new online collaboration tool into their course, which requires students to provide their personal information when they sign up.

c) Why is a PIA Required?

PIAs are not just good business practice; they are a requirement under BC's Freedom of Information and Protection of Privacy Act (FOIPPA). Non-compliance with the requirement to conduct PIAs have legal consequences.

d) How Can I Confirm if my Project Requires a PIA?

If you have a new initiative or a modification to existing initiatives at UNBC, you must consult with the UNBC Privacy and Access team to determine whether a PIA is required. Initiate the PIA process by contacting the privacy office at privacy@unbc.ca.

6. Vendor Management

a) Privacy and Security Assessment of Contracts

When engaging with an external vendor who will access, process or store personal information, we must ensure, as mandated by FOIPPA, that the vendor safeguards the information to a standard comparable to UNBC's.

Before entering a contract with a new vendor, notify the Privacy and Access team via email at privacy@unbc.ca. If the vendor requires the use of personal information, UNBC needs to ensure that a Privacy Schedule is executed. Furthermore, the Privacy and Access team needs to determine if a Privacy Impact Assessment (PIA) or a Security Risk Assessment (SRA) are necessary.

Even if a vendor is offering a free service that requires personal information, it is important to engage the Privacy and Access team to ensure the appropriate agreements are in place to safeguard the personal information.

ADDITIONAL RESOURCES

UNBC Resources:

- **Protection of Privacy Policy**
- **Record Management Guidelines**
- **UNBC PIA Process Flow**

External Resources:

- **FOIPPA**
- **BC's Guide to Good Privacy Practices**