



Employee Confidentiality

Category:	Employment.
Number:	
Audience:	All Employees
Issued:	September 22, 2018
Owner:	President
Approved by:	Board of Governors
Contact:	Vice President Finance and Administration

Introduction

The First Nations University of Canada (the University) is committed to upholding the highest standards of ethical behavior. The intent of this policy is to define and describe the management of confidential information by employees of the University.

University employees receive and generate on behalf of the University various types of confidential, proprietary and private information. It is imperative that each university employee complies with all federal laws, provincial laws, agreements with third parties, and University policies and principles pertaining to the use, protection and disclosure of such information.

This policy applies to all employees of the University during the term of their employment and beyond the time that the University employee's relationship with the University ends.

Definitions

Breach: A breach is when confidential information is accessed, shared, or disclosed, in any format (oral, printed, or electronic), by an individual for any purpose other than which they are authorized.

Confidential Information: Confidential information includes any information, whether oral, printed, or electronic that is generated or accessed through the course of employment and is not rightfully, legally or ethically shared in the public domain outside of the University environment. This includes, but is not limited to,; personal, financial, and technical information; management policies; student records, financial records, human resources/payroll information, legal documents, and research data.

Employees: This includes, but is not limited to, any full or part-time permanent, term or casual faculty or staff member and any person who teaches, conducts research, adjunct and sessional faculty members, librarians, program directors, post-doctoral fellows, emeriti, visiting professors, contractors, students, Board members and volunteers

Personal Information: This includes, but is not limited to, a person's first name or first initial and last name in combination with identifying information such as Social Insurance Number, driver's license number, income, financial history, banking information, credit card numbers, contact information, date of birth, gender, marital status, race citizenship, education, employment history, or criminal history.

FIRST NATIONS UNIVERSITY OF CANADA

Personal information does not include information that an individual has consented to, in writing, have publicly disseminated or listed.

Supervisor: A person authorized by the University to oversee or direct the work of employees, including research supervisors, principal investigators, department heads, managers and any other person in positions of authority.

Policy

All confidential information must be maintained in a manner that ensures confidentiality. Confidential information must be used or reviewed on a strict need-to-know basis in the performance of job functions and must not be disclosed to anyone other than persons authorized to receive it. All employees shall not, during their employment or any time after the termination thereof, disclose confidential information to any person or organization.

Employees who are authorized to use or disclose confidential information also have the responsibility to safeguard access to such information. Access to this information must be appropriate to the employee's job responsibility. Employees who are uncertain whether information is confidential must check with their supervisors and any other appropriate University authorities before using and disclosing it.

Any suspected, mistaken, or inadvertent confidentiality breach related to privacy or personal information must be immediately disclosed to the employee's supervisor and appropriate University officials to determine the University's response and actions. The team members and the supervisor should:

- Determine the nature of the unauthorized disclosure;
- Take immediate steps to stop, limit, or mitigate the breach; and
- Gather any other relevant information.

Employees shall sign and abide by a Confidentiality Agreement to be kept in their employee file.

Role and Responsibilities

All employees shall comply with this policy and will sign a Confidentiality Agreement, to be kept in their employee file. Employees are responsible for safeguarding confidential information and must take all reasonable steps to prevent the disclosure of such information and to inform their supervisor and the Vice President Finance and Administration of any suspected breaches of this policy, related procedures, and relevant legislation.

Consequences for Noncompliance

All employees of the University are subject to the requirements of this policy. The release of any such confidential information may result in negative or financial action, productive loss, or cause legal or other non-beneficial impacts on the University. Violations place the University at significant risk and employees are subject to disciplinary action up to and including termination.

This policy is binding even after separation of employment.

Related Information

Identify related documents/information (acts, regulations, policies, strategies, procedures, forms, etc.)

- Confidentiality Agreement
- Respectful University Policy
- *The Freedom of Information and Protection of Privacy Act*