

NSAC Policy for the Protection of Personal Information from Access outside Canada

Purpose

The purpose of this policy is to assist NSAC in meeting the legal obligations under the 2006 *Personal Information International Disclosure Protection Act* (PIIDPA). It also helps us meet our obligations to all members of the university community (students, faculty, staff and alumni) and to participants in university research and international projects to protect their personal information from unauthorized access outside Canada. This policy is supplementary to other university regulations, policies, and guidelines concerning the administration and release of student, employee and alumni information and concerning the administration and approval of research projects.

Definitions

“Personal information” means recorded information as defined in the FOIPOP Act about an identifiable individual, including, but not limited to:

- a. name, address, telephone, email (personal not business);
- b. race, ethnic origin or religious political beliefs or associations;
- c. age, sex, sexual orientation, marital status or family status;
- d. any identifying number or symbol (examples: Student ID, SIN, credit card, health insurance, drivers' license);
- e. fingerprints, blood type, or inheritable characteristics;
- f. medical or personal history;
- g. educational, employment, financial, or criminal history;
- h. personal views or opinions.

Data repository means any medium or device (e.g. disk drive, memory stick, CD, DVD, computer, laptop, PDA, Blackberry) where data is recorded, including but not limited to, databases, spreadsheets, paper and electronic documents;

Employees, for the purposes of this policy include university employees, academic appointees, and individuals engaged to work on NSAC research or other projects;

University data repository means a data repository that is owned or controlled by NSAC or utilized in research or other projects under the direction of a faculty or staff member.

Policy

1. All university data repositories that store personal information shall be housed and backed-up in Canada unless:
 - a) There is no product or service that permits the storage, housing or backup of the personal information in Canada that meets the purchasing requirements in a competitive manner, having regard to the overall cost, range of services or functions, degree of sensitivity of the personal information at issue, data security arrangements, and whether it is necessary to meet the requirements of a university program, operation or activity;

2. Employees who wish to purchase a product or service under section 1 must obtain prior written approval of the Vice-President Administration. The employee making the purchase or request for services shall submit a completed approval form to the Vice President Administration for signature. No purchase or service request shall be made until the approval is complete.

Disclosure of or Access to Personal Information from Outside Canada

3. Personal information held on NSAC data repositories shall not be disclosed to any person or organization outside Canada unless:
 - a) The disclosure or access is to the individual's own information; or
 - b) The individual has consented to the disclosure, such consent to be in a form approved by the Vice-President Administration; or
 - c) The disclosure is necessary for completing financial transactions under the direction of Financial Services (eg. processing of cheques, drafts, credit card or other forms of payment by, and to the credit of, the university); or
 - d) Such disclosure is otherwise approved in advance in writing by the Vice-President Administration; or
 - e) As required by law.

Transporting Personal Information Outside Canada

4. Employees may transport personal information temporarily outside Canada or access it over the Internet only to the extent that it is strictly necessary for their assigned duties or as a necessary part of a research or other project. In such event, employees are required to take all reasonable precautions to protect the personal information. Questions on transport of personal information should be directed to the NSAC FOIPOP coordinator.

Requests for Disclosure of Personal Information

5. Any requests for disclosure of personal information by authorities or organizations from outside Canada, or which have the appearance of being from such sources, shall be referred to the Vice-President Administration as soon as reasonably possible following receipt of such a request.

Notification of Unauthorized Disclosure

6. Any known or suspected unauthorized disclosure of personal information as outlined by this policy must be reported as soon as possible to the Vice-President Administration.

Approval Form

APPROVAL TO PURCHASE SOFTWARE OR SERVICE THAT STORES OR BACK-UP PERSONAL INFORMATION OUTSIDE OF CANADA OR FOR MAINTENANCE SERVICES PERMITTING REMOTE ACCESS FROM OUTSIDE CANADA

Indicate what type of personal information the product will be used to house, store or back-up (check all that apply):

- Name, address, telephone, email (personal, not business)
- Race, ethnic origin or religious political beliefs or associations
- Age, sex, sexual orientation, marital status or family status
- Any identifying number or symbol (examples: Student ID, SIN, credit card, health insurance, drivers' license)
- Fingerprints, blood type, or inheritable characteristics
- Medical or personal history
- Educational, financial, criminal or employment history
- Personal views or opinions
- Other (define)

PLEASE NOTE: If the above information is not linked to an identifiable individual then approval is not necessary.

Name of company/firm and name of international affiliations:

(Give the full name of the company, place of operation(s), whether owned or part of an international group of companies – you should ask the company/firm for this information)

Product/service name and purpose/function:

(Give the name of the product or service and briefly describe its purpose.)

University program, operation, activity or research project:

(Describe the program, operation, activity or research project that the product or service is to support and what value it adds to that program, operation, activity or research project. In the case of research projects, please indicate whether ethics approval has been granted.)

Other similar products or services available in Canada? Yes ___ No ___

If no, describe the process undertaken to support this conclusion:

If yes, why is this product superior?

(Please address comparative cost, range of service, functionality, other relevant factors)

What security measures are proposed to protect the personal information?

(Provide details concerning the security of the system as well as contractual measures taken to protected against or reduce unnecessary access to personal information)

Has the contract been reviewed by the FOIPOP Coordinator? Yes ___ No ___

Name: _____

Department: _____

University Approval:

Vice-President Administration