B5001 – PRIVACY AND ACCESS

PROCEDURES

1. Protecting Privacy

1.1 General

College administrators will determine the level of access to personal information that employees and service providers working in their departments need to perform their duties.

Administrators will ensure that paper and electronic forms and data entry screens used to collect personal information from students, alumni, employees and others include a notice to inform the individual of:

- the College's legal authority for collecting the information;
- the purpose for its collection;
- how it will be used; and
- the position and contact information of the person who can answer questions about its collection.

See Appendix I for a sample of a collection, use and disclosure of personal information notification.

Administrators in the Information Technology (IT) and Educational Technology (EdTech) departments will establish policies, procedures or guidelines to protect personal information maintained on the College's computer systems from unauthorized collection, access, use, disclosure, storage or disposal.

Departments that finalize the purchase of goods or services or finalize contracts and agreements that involve the collection, use, disclosure or storage of personal information will ensure the inclusion of privacy protection provisions that meet *Freedom of Information and Protection of Privacy Act* (the Act) requirements.

1.2 Information Sharing Agreements (ISA)

Before departments begin any initiative that involves the College and another organization jointly collecting, using and/or disclosing students' personal information, administrators and the other party's representative will complete an Information Sharing Agreement with the assistance of the Registrar and Records Management and Privacy. The ISA, which both parties approve, sets out conditions for their collection, use and/or disclosure of personal information. Records Management and Privacy will maintain a permanent file of completed ISA's.

1.3 Privacy Impact Assessments (PIA)

Before departments develop, implement or change any program, system or initiative that involves personal information, especially those that use cloud computing services, administrators will complete a checklist to identify potential privacy impacts. Records Management and Privacy will review the checklist. If the privacy impacts are significant, Records Management and Privacy will complete a comprehensive Privacy Impact Assessment with the assistance of departmental subject matter experts as well as the Information Technology or Educational Technology departments, as applicable. Department administrators and a member of the Senior Leadership Team are responsible for approving Privacy Impact Assessments. Records Management and Privacy will maintain a permanent file of completed checklists and PIA's.

2. Providing Access to Information

2.1 Responding to Requests for Routinely Available Information

Department administrators and Records Management and Privacy will work together to identify the types of College recorded information and personal information that the department routinely makes available upon request, and establish access procedures or guidelines.

Employees who receive a request for College recorded information or personal information will confirm that the department has listed it as being routinely available and provide it to the requester without delay.

2.2 Responding to Requests for Information Not Routinely Available

Employees who receive a request for College recorded information or personal information that is not routinely available will refer the request to a department administrator who will consult with Records Management and Privacy to determine if the Act authorizes the release of information.

Service providers who receive a request for College recorded information or personal information will refer the request to an administrator familiar with the operations of the department and the records it maintains.

Records Management and Privacy will process most requests for access to information, including personal information, according to the Act's procedures and timelines. However, other departments, such as Registrar and Enrolment Services, may process certain types of requests, e.g., hiring agencies and employers requesting student credential information or program status.

2.3 Third-Party Requests for Personal Information

Administrators will develop consent forms for students to complete to authorize the release of their own personal information to their parents, guardians or others. Departments will retain the completed consent form in the student's file. *See Appendix II for a sample of a consent to release personal information form.*

Departments that receive written requests from third parties not listed on a consent form on file, such as law firms or insurance companies, will forward the request, the individual's authorization form and the requested records to Records Management and Privacy for processing, without delay.

When Records Management and Privacy receives a written request from a third party for personal information with the person's written authorization, it will request the records from the appropriate department and provide a copy of the letter and authorization, without delay.

Employees who receive verbal requests from external third parties for the personal information of students or other employees will not provide the requested information without first obtaining the individual's written authorization. In specific situations, such as when the health and safety of the person or of other people is at imminent risk, employees may need to disclose personal information without written authorization.

2.4 Personal Information Banks

As required by the Act, Records Management and Privacy will maintain a Directory of Personal Information Banks and make it accessible to the public. A personal information bank is a

collection of personal information that is organized or retrievable by a person's name or by an identifying number, symbol or other particular assigned to the person. The Directory will include the following for each personal information bank:

a) its title and location;
b) a description of the kind of personal information and the categories of persons included in the bank;
c) the authority for its collection;
d) the College's purposes for obtaining or compiling the information and the purposes for using or disclosing it; and
e) the categories of persons who use the bank or to whom it is disclosed.

3. Privacy and Access Training, Services and Resources

3.1 Records Management and Privacy will provide privacy and access-related training, services and resources to employees and service providers that ensure uniform privacy protection and access to information practices across the College including, but not limited to:

- Presentations, tutorials and quizzes
- Privacy impact checklists and assessments
- Contract and service agreement reviews
- Ad hoc consultation and advice.

4. Investigating Unauthorized Disclosures and Breaches of Personal Information

4.1 When employees and service providers discover an unauthorized disclosure of personal information they must immediately contact the President or designate.

4.2 Records Management and Privacy, Organizational Risk Assessment and, when applicable, Information Technology or Educational Technology will coordinate investigations of unauthorized disclosures and breaches of personal information.

4.3 These departments will conduct investigations with the assistance of other department resources as necessary, to

- identify the source and extent of the breach and take immediate steps to contain it by:
    a) stopping the unauthorized practice;
    b) shutting down the system;
    c) recovering lost records or data; and/or
    d) revoking system access.
- analyze the cause of the breach and identify measures to prevent similar incidents in the future.
- determine whether the breach will cause harm to anyone involved, such as identity theft, financial loss or risk to personal safety.

4.4 Records Management and Privacy will submit a report on the incident and subsequent investigation to the Senior Leadership Team and, as appropriate, to the Office of the Information and Privacy Commissioner.

4.5 The Senior Leadership Team will decide whether to notify individuals who may be harmed by the breach.

Appendix I – Sample Collection, Use and Disclosure of Personal Information Notification

Langara College collects the information on this form under the authority of the College and Institute Act [RSBC 1996, Chapter 52, Section 41.1]. This information is needed, and will be used, for purposes that are consistent with activity necessary to the operation of the College and in compliance with the provisions of the Freedom of Information and Protection of Privacy Act [RSBC 1996, Chapter 165]. This information will be used for admission, registration, and maintenance of your student record. Information is shared with College Advancement, Alumni Relations, and the Langara Students' Union.

The personal information you provide on this form may be shared with the Ministry of Education and will be used to verify your British Columbia Personal Education Number (PEN) or assign one to you. The personal information you provide and your PEN are used for authorized statistical and research purposes only.

Some courses may require students to use electronic instructional resources where students log in by entering personal information, such as name and email address, which is then stored on servers outside Canada.

For questions about the collection, use and disclosure of your personal information, contact the Registrar at 604-323-5241.

Excerpted from Application for Admission Form

Appendix II – Sample Consent to Release Personal Information Form

Langara.
THE COLLEGE OF HIGHER LEARNING.

Consent for Authorized Representative
Registrar & Enrolment Services

STUDENT INFORMATION

LANGARA ID: _____ DATE OF BIRTH (MM/DD/YYYY): _____

LEGAL SURNAME: _____ LEGAL FIRST NAME: _____

REPRESENTATIVE INFORMATION

FULL NAME OF PERSON/AGENCY: _____

RELATIONSHIP: _____ EMAIL*: _____

* Information will only be shared with this representative in person and/or by email. If you do not wish for information to be shared by email, please leave this field blank. Email inquiries will only be responded to if sent from this address.

This waiver will be valid for the following period, or until I revoke authority:

From: _____ To: _____

STUDENT INFORMATION

I authorize the person/agency stated above access to the following information:

- ☐ Academic standing
- ☐ Application status
- ☐ Final grades
- ☐ Graduation requirements
- ☐ Registration information (including current registration status)
- ☐ Special needs documentation or disability accommodations
- ☐ Other (specify): _____

FINANCIAL INFORMATION

I authorize the person/agency stated above access to the following information:

- ☐ Student account balance
- ☐ Student awards
- ☐ Student loan information
- ☐ Tuition and fees assessment
- ☐ Other (specify): _____

STUDENT TRANSACTIONS

I authorize the person/agency stated above to carry out the following transactions on my behalf:

- ☐ Order transcripts, confirmation of enrolment letters, RESP forms, etc.
- ☐ Pick up transcripts, confirmation of enrolment letters, RESP forms, etc.
- ☐ Other (specify): _____

CONDITIONS

1. I understand that the Authorized Representative is permitted to represent me up to and including the end date I have selected.
2. I understand that Langara College collects, uses and discloses my personal information in compliance with the provisions of the British Columbia Freedom of Information and Protection of Privacy Act [RSBC 1996, Chapter 152] and will use the information for research and statistical purposes subject to the provisions of the Act.
3. I understand that if I wish to extend the authorization period I have selected above, it is my responsibility to submit a new Consent for Authorized Representative form.
4. I understand that any request to cancel this authorization before the end date I have selected above must be submitted in writing.
5. I understand that if I have already submitted a Consent for Authorized Representative form, this form overrides the previous one.
6. I have read and understood the above statements.

STUDENT'S SIGNATURE: _____ DATE: _____

SUBMIT COMPLETED FORM

In person to: Registrar & Enrolment Services, Langara College, 100 West 49th Ave., Vancouver, BC V5Y 2Z6

J:\STUDENT\Graduation and Publications\Publications\Forms\Consent for Authorized Representative 08/2016

Appendix III – Guidelines for Protecting Personal Information

1. Receive and return student work in a way that protects students' personal information from being disclosed to others. Such records include assignments, tests or other documents that include a student's name, identification number, physical address, e-mail address, telephone number or other personal identifier.

2. Do not put student records, such as completed assignments, or employee records that contain personal information in publicly accessible places, including holders outside office doors.

3. Keep a 'Clean Desk' policy. Whether working remotely or in the office, remove any records that contain personal information from your desk or printer when you leave your work area and place them in a lockable drawer or file cabinet.

4. Protect and secure records that contain personal information on computers, laptops, portable storage devices and mobile devices by using passwords, encryption, privacy screens or other security measures. Lock your computer when you leave your work area, even if it's just for a moment. Delete any records that contain personal information when they are no longer required to support College operations.

5. Send personal information by e-mail, fax machine or other electronic means only to the individual it concerns and request recipients to keep the information secure.

6. Do not use your personal email to transfer records containing work-related personal or confidential information.

7. Do not forward electronic communications to any personal accounts or servers, including, but not limited to, personal webmail (such as GMail, Yahoo, etc.) or document storage services (such as Dropbox).

8. Securely dispose of records that contain personal information according to retention schedules approved by the College.

9. Deposit paper records that contain personal information in confidential destruction bins located throughout the College, or use department/home shredders. Do not use recycling containers either at work or at home.