CAPILANO UNIVERSITY	POLICY		
Policy No.	Officer Responsible		
B.700	**Vice President, Finance & Administration**		
Policy Name			
Privacy and Access to Information			
Approved by	Replaces	Category	Next Review
Board	**New**		February 2025
Date Issued	Date Revised	Related Policies and Procedures	
February 2023		OP.604 Acceptable Use and Security of IT E.210 Surveillance Policy OP.606 Student Records Management and Access E.301 Development and Alumni Relations – Data Management B.700.1 Personal Information Incident Management Procedure B.700.2 Right to Request Correction Procedure	

1 PURPOSE

1.1 To put in place reasonable and required measures to safeguard personal information in the custody or control of Capilano University "the University" in compliance with the *Freedom of Information and Protection of Privacy Act* (FIPPA). This will give Employees and Students the confidence that their personal information will be handled and protected appropriately by the University. In the event of any conflict between this policy and FIPPA or other applicable law, the legislation will govern.

1.2 This policy describes how the University will:

a. protect the personal information of Students, employees, volunteers, donors, alumni and other people who interact with the University "Individuals" in the University's custody or control;
b. enable Individuals to access and make corrections to their personal information; and
c. provide the public with the right of access to general information in its custody or under its control.

2 DEFINITIONS

Confidential Information is information that becomes available to an employee as a result of their employment and is not otherwise generally available. Confidential information includes business, proprietary, technical, operational, financial, and legal, as well as personal information relating to employees or Students.

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.

Control (of a record) means the power or authority to manage the record throughout its life cycle, including restricting, regulating, and administering its use or disclosure.

Custody (of a record) means having physical possession of a record, even though the public body does not necessarily have responsibility for the record.

Disclosure means making personal information available to a third party.

Employee means any person employed by the University.

Freedom of Information request or **FOI request** are public requests for access to information in University records, which may contain personal or confidential information.

General Information is recorded information that is not personal information.

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

Personal Information Incident means an incident as defined in the Personal Information Incident Management Procedure.

Records include books, documents, maps, drawings, photographs, audio or video recordings, letters, papers, and any other thing on which information is recorded or stored by graphic, electronic, mechanical or any other means, but does not include a computer program or any other mechanism that produces records. Records include email and information stored electronically. Records created and received by University officers and employees in the course of their duties on behalf of the University belong to the University and are subject to FIPPA.

Student means an individual enrolled in any course (credit or non-credit) at the University.

Student Records means recorded information that is personally identifiable or traceable to the student. Student records include, but are not limited to:

a. academic records;
b. registration status;
c. awards and distinctions; and
d. programs of study.

Third party means a person, group of persons, or an organization other than the individual the information is about. An employee of the University, acting in their official capacity, is not considered a third party.

3 SCOPE

3.1 This policy applies to:

a. Personal Information in the custody or under the control of the University; and
b. to all University Employees, volunteers, service providers and their subcontractors (e.g., persons or corporate entities retained under a contract to perform services for the University)

3.2 This policy does not impose any limits on the collection, use or disclosure of the following information:

a. business contact information;
b. information collected, used, or disclosed for journalistic, literary, or artistic activities; and
c. aggregate information that cannot be associated with an identifiable person.

4 POLICY STATEMENT

4.1 All public bodies are required to collect, use, disclose, retain, and protect Personal Information in a lawful and appropriate manner. The University manages Personal Information in accordance with its obligations under FIPPA, the *University Act*, collective agreements, contracts, other applicable University policies and procedures and other applicable law.

4.2 When the University engages in extra territorial activities, compliance with international privacy regulations such as the California Consumer Privacy Act (CCPA) or the General Data Protection Regulation (GDPR) will be taken into consideration, to the extent of applicability.

4.3 The University collects, uses, discloses, and maintains Personal Information for the purposes of admission, registration, instruction, Student care and support, research, alumni relations, and other activities related to the management of a BC post-secondary institution pursuant to the *University Act* and FIPPA.

4.4 Over the course of their duties, Employees may have access to and are entrusted with Confidential and Personal Information. Employees are responsible for maintaining the complete confidentiality of all University and third-party Confidential and Personal Information and must not disclose it to anyone inside or outside the University except as permitted or required by law.

4.5 Only those Employees of the University who require access while performing their official University duties are granted access to Personal Information about Individuals who interact with the University. Access to Personal Information will be granted on a need-to-know basis, which must be consistent with the original purpose for collection. University Employees will be asked to sign a Confidentiality and Release of Information Agreement upon joining the University.

5 ROLES AND RESPONSIBILITIES

5.1 The Vice President Finance and Administration (VP) is responsible for:

a. implementing, administering and ensuring compliance with this policy and any related procedures that together comprise the University's privacy management program; and
b. appointing a Privacy Officer to co-ordinate privacy and access functions and be the point of contact for privacy related matters.

5.2 The Privacy Officer is responsible for:

a. providing privacy advice and training and awareness raising activities;
b. providing ongoing assessment of privacy risks including facilitating Privacy Impact Assessments;
c. making sure mechanisms to inform service providers of their privacy obligations are in place;
d. coordinating investigations and responses to Personal Information Incidents;
e. responding to privacy complaints and investigating concerns about privacy issues; and
f. developing and monitoring the privacy management program.

5.2 Senior Leaders and Administrators are responsible for making sure that their faculties or departments:

a. collect only those items of personal information that are necessary to fulfill legitimate University operations;
b. obtain explicit and specific consent when personal information is collected unless expressly required or authorized by applicable law;
c. put in place reasonable security arrangements around personal information under their area of control (for example the use of locked filing cabinets, orientation of screens etc.);
d. direct Employees for whom they are responsible to this policy and any training or awareness materials provided, so that they are aware of and understand their responsibilities under this policy and seek advice when they are not certain of their obligations;
e. inform all Students acting in designated roles within university processes (for example on hiring committees, Student appeals processes) or volunteers who may have access to personal information in their voluntary role that support the areas work of their privacy responsibilities;
f. confirm that contracts or agreements for which they are responsible include a Privacy Protection Schedule;

g. initiate Privacy Impact Assessments prior to undertaking new systems, projects, programs or activities that involve the collection, use or Disclosure of Personal Information;
h. report any Personal Information Incidents (privacy breaches) to the Privacy Officer;
i. implement the recommendations of the Privacy Officer following a Privacy Impact Assessment or resulting from the investigation of a Personal Information Incident or complaint; and
j. provide records to the Privacy Offer as requested within agreed deadlines to fulfil Freedom of Information requests.

5.3 Employees are responsible for:

a. Handling all Personal Information to which they receive access in accordance with the Act and this policy;
b. Accessing Personal Information only as necessary for the performance of their duties; and
c. Reporting any suspected or actual Personal Information Incidents to their supervisor, manager, chair/coordinator, or administrator or directly to the Privacy Officer in accordance with the University's Personal Information Incident Management Procedure.

5.4 Third Party Service Providers

The University will require Third Party service providers whose work on behalf of the University involves the collection, use or Disclosure of Personal Information to sign and abide by the Privacy Protection Schedule in the handling of Personal Information on behalf of the University, and may require confidentiality agreements to be signed.

6 PROTECTION OF PERSONAL INFORMATION

6.1 COLLECTION

6.1.1 The University collects Personal Information from Students, Employees, volunteers, alumni, donors, or other individuals for the following purposes:

a. in order to fulfill its mandate under the *University Act*
b. for University programs and activities, including information necessary to:
    i. establish and maintain responsible relations with Students, donors, and alumni, and to provide ongoing service
    ii. understand Students' needs
    iii. manage and develop University operations, including personnel and employment matters
c. to meet legal or regulatory requirements

6.1.2 The University will collect Personal Information directly from the individual the information is about, but may collect Personal Information indirectly in limited situations for the purpose of:

a. determining suitability for an honour or award (eg a scholarship, prize or bursary);

b. a proceeding before a court or a judicial or quasi-judicial tribunal;

c. collecting a debt or fine or making a payment;

d. law enforcement;

e. any other purposes permitted by law; or

f. if authorized by the individual.

6.1.3 The University will provide notice to the individual of the purposes to which it collect, uses or shares the Personal Information, except where otherwise authorized or required by applicable law.

6.1.4 Where Personal Information is collected, used or disclosed in order to provide services this will be explicitly stated as a condition of service. Where additional information is collected, used, or disclosed an opt in or opt out choice will be given.

6.2 USE

6.2.1 The University uses the Personal Information in its Custody or under its Control only:

a. for the purpose for which that information was collected or for a use consistent with that purpose;
b. with notice to and consent of the individual the Personal Information is about; or
c. for other purposes permitted or required by applicable laws.

6.2.2 Personal Information at the University is shared internally on a need-to-know basis. Employees must only access and use Personal Information necessary for the performance of their duties. Employee access to and use of Student Records is also subject to policy OP.606 Student Record Access and Management.

6.2.3 The University is subject to Canada's Anti-Spam Legislation (CASL), which places restrictions on sending unsolicited electronic messages that are "commercial" in nature. Any University departments that engage in marketing will put in place procedures to govern their activities accordingly, including:

a. collection of express consent;
b. approval of message scripts;
c. making sure that unsubscribe requests are actioned in a timely manner;
d. monitoring and complaints mechanisms; and
e. training for team members.

6.3 DISCLOSURE

6.3.1 The University treats Personal Information in its Custody and under its Control with a high degree of confidentiality. The University will not disclose Personal Information about Students or Employees to any Third Party unless it is otherwise provided for under applicable law or with the express consent of the individual.

Disclosure of the following information without consent is generally permitted, however Employees who have questions should seek guidance from the Privacy Officer:

a. Information about an individual's position, function or remuneration as an Employee of the University as permitted under FIPPA;
b. Names of individuals who have received degrees, the names of degrees those individuals have received and the years in which the degrees were awarded;
c. Personal Information about a Student in an emergency or where the Registrar and/or the Vice-President Academic & Provost determine that compelling circumstances exist that affect anyone's health or safety; and
d. Personal Information about an individual other than a Student in an emergency or where the Vice-President Finance and Administration determines that compelling circumstances exist that affect anyone's health or safety.

6.4 ACCURACY OF FACTUAL INFORMATION

6.4.1 The University will make every reasonable effort to ensure that the Personal Information in its custody or under its control is as accurate and complete as is necessary for the purpose for which it was collected.

6.4.2 In accordance with the Right to Request Correction Procedure, the University will correct or annotate the personal information of an individual upon request in accordance with FIPPA.

6.5 PROTECTION AND SAFEGUARDS

6.5.1 The University will make reasonable security arrangements to prevent the risk of unauthorized collection, access, use, disclosure, or disposal of Personal Information.

6.5.2 The University will ensure that 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.

6.6 RETENTION AND DISPOSITION

6.6.1 The University will retain Personal Information only if it remains necessary or relevant for the identified purposes, as required by University policies, or as required by applicable law. Depending on the circumstances, where Personal Information has been used to make a decision about an individual, the University will retain, for at least one year or a period of time that is reasonably sufficient to allow for access by the individual, either the actual information or the rationale for making the decision.

6.6.2 Destruction of records containing Personal Information will occur in accordance with University policies and procedures.

7 ACCESS TO INFORMATION

7.1 The University supports the public's right of access to General Information and the individual's right of access to Personal Information about themselves in accordance with FIPPA.

7.2 Individuals have the right of access to records containing their own Personal Information. The University will put in place self-serve mechanisms where possible to enable Individuals to access their own Personal Information. Access fees will not be charged to Students or employees to access personal information with the exception of copies of transcripts.

7.3 The following types of information records can be requested informally through routine channels:

a. A record that does not contain personal information about a Third Party and that only contains personal information about the individual making the request (such as a Student requesting copy of their own transcript); and
b. Personal Information released to a Third Party with a signed and dated consent form from the individual to whom the information relates naming the individual who may be given access if there is no other third-party information included.

7.4 Other information may be requested through the use of a Freedom of Information Request. FOI requests are processed by the Privacy Officer and subject to Disclosure limitations under FIPPA. Information excepted from Disclosure under sections 12 to 22 of FIPPA will be redacted. Fees may be charged for copying and if the time spent locating and retrieving records exceeds three hours an additional hourly fee may be charged in line with Schedule 1 of the FIPPA Regulation.

7.5 Access to Student Records is subject to policy OP.606 Student Records Management and Access.

8 CHALLENGING COMPLIANCE

8.1 Individuals have the right to complain to the University and/or to the Office of the Information and Privacy Commissioner if they believe their privacy has been breached.

8.2 The University promotes a culture that values complaints and their effective resolution and encourages Employees to be alert to complaints and resolve them promptly.

8.3 Privacy related complaints that cannot be resolved informally should be referred to the Privacy Officer to manage.

9 REPORTING

9.1 All University Employees have a duty to report Personal Information Incidents to their supervisor or manager in accordance with the Personal Information Incident Management Procedure.

9.2 The Privacy Officer will:

a. report on overall compliance with FIPPA and the University's privacy management program including this policy and associated procedures;
b. report on all Personal Information Incident Management investigations;

c. provide regular reports to the Vice President, Finance and Administration about complaints relating to the management of Personal Information (both to the University and about the University), and on issues arising from privacy complaint handling work; and
d. Recommend changes in practice identified as needed through investigations of Personal Information Incidents and privacy related complaints, and follow up to make sure agreed improvements are made.

10 DESIGNATED OFFICER

The Vice President, Finance and Administration is the Policy Owner, responsible for the oversight of this Policy. The Administration of this Policy and the development, subsequent revisions to and operationalization of any associated procedures is the responsibility of the designated Privacy Officer.

11 ASSOCIATED GUIDANCE

Privacy Guidelines for Employees
Privacy Impact Assessment Guide
Confidentiality and Release of Information Agreement

12 REFERENCES AND PROFESSIONAL STANDARDS

Freedom of Information and Protection of Privacy Act
Freedom of Information and Protection of Privacy Regulations
Government of British Columbia Guide to Good Privacy Practices
Office of the Information and Privacy Commissioner for British Columbia