KPU | KWANTLEN POLYTECHNIC UNIVERSITY

Policy History
Policy No. IM8
Approving Jurisdiction: President
Administrative Responsibility: President
Effective Date: November 30, 2022

Privacy
Procedure

A. DEFINITIONS

1. **Fair Information Principles:** a set of generally accepted privacy principles that create restrictions, requirements, and accountability related to the collection and processing of Personal Information by an entity. The majority of FIPs applicable to the University are reflected in FIPPA.
2. **FIPPA (or "the Act"):** Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, Chapter 165 - including FIPPA Regulations, related Orders in Council, and any Orders/Directions of the Minister responsible for the Act.
3. **Manager, Information Access and Privacy:** University Employee tasked with coordinating the University's compliance with FIPPA.
4. **Office of General Counsel:** the University's internal legal department.
5. **Personal Information**: Under FIPPA, Personal Information is recorded information (see "Records" below) about an identifiable individual, excluding "Contact Information" as defined in FIPPA; that is, information to enable an individual at a place of business to be contacted. Personal Information which, either alone or in combination, could reveal the identity of an individual includes name; home address; personal telephone number; email address (including University email address in the case of applicants/students); date of birth; age; sex; gender; sexual orientation; marital/family status; religious or political beliefs or associations; photo; video or voice recording; financial information, including credit card number, financial assistance, or scholarship information; medical, psychiatric or psychological information, including disability accommodation information or counselling notes; educational history, including grades, transcripts, preferred course of study, course work, or student conduct decisions; employment history, including performance management plans or disciplinary records; donation history or commitments; biometric data; racial or ethnic origin; reflections, thoughts or feelings; any identifying number or symbol assigned to an individual; IP address, personal computing device information, browsing history. The foregoing are illustrative examples and is not an exhaustive list. See also Sensitive Personal Information below. Under this Policy, privacy considerations extend to non-recorded Personal Information.
6. **Privacy Advice or Guidance:** privacy-related recommendations or instructions provided verbally or in writing by the Manager, Information Access and Privacy, designate, or Office of General Counsel for a specific query.

7. **Privacy Breach:** The unauthorized collection, use, or disclosure of or access to Personal Information in contravention of Part 3 of FIPPA and that invokes the Privacy Breach Protocol. Privacy breaches may be external or internal to the University.
8. **Privacy Breach Protocol:** a defined set of steps to respond to a Privacy Breach, including activities related to containment, risk evaluation, notification, and prevention.
9. **Privacy Complaint:** a report of dissatisfaction (that may or may not follow a Privacy Breach) with how the University manages or processes Personal Information.
10. **Privacy by Design:** a proactive approach to ensuring privacy is embedded as a core element in the development of University Initiatives and practices to protect Personal Information prior to its collection and through the information lifecycle to disposal, and to creating a privacy culture at the University.
11. **Privacy Guideline:** a written document provided by the Manager, Information Access and Privacy, designate, or Office of General Counsel providing guiding principles for making privacy-related decisions.
12. **Privacy Impact Assessment (PIA):** an evaluation of privacy implications of a University Initiative in accordance with FIPPA and this Procedure.
13. **Privacy Incident:** an event involving potential mishandling of Personal Information that does not meet the criteria of a Privacy Breach. (Note: A Privacy Incident may, upon investigation, be deemed a Privacy Breach.)
14. **Privacy Protocol:** a prescriptive set of instructions or practices about a privacy-related topic.
15. **Privacy Risk:** probability of actual or potential harms (to an individual or the University) related to a University Initiative involving Personal Information in the University's custody or control.
16. **Records:** anything on which information is recorded or stored by graphic, electronic, mechanical or other means, including emails, books, documents, maps, drawings, photographs, letters, notes, vouchers, papers, audio or video recordings, etc. These include any records within the scope of FIPPA in the custody or control of the University including all types of student records, University Employee records, and records of other University constituents. Records outside the scope of FIPPA include Teaching and Research Materials, as defined below. (Please note: the following definitions are for guidance only; they are not exhaustive and all exceptions are not listed.)
    a. Teaching Materials: include records produced or compiled for distribution to students, to aid an instructor in relating information to students, or otherwise used to teach. Example: notes prepared by a university professor to refer to while presenting a lecture to students. (Exceptions: "Teaching Materials" do not include communications with students; students' completed/graded assignments; instructor/course/program evaluations; or performance reviews, which would be within the scope of FIPPA.)
    b. Research Materials: includes records related to academic research that are typically subject to compliance with relevant research ethics requirements (i.e. TCPS2). (Exceptions: "Research Information" does not include quality assurance and quality improvement studies related to the University's policies, practices, and services, which would be within the scope of FIPPA.)
17. **Sensitive Personal Information:** A subset of Personal Information, Sensitive Personal Information is context dependent and requires special consideration under the Act. Sensitive Personal Information may include data elements revealing medical/health conditions, ethnic and racial origins, political opinions, genetic and biometric data, gender or sexual orientation, religious/philosophical beliefs, and many others. An individual piece of information considered non-sensitive on its own, could become sensitive depending on what it may reveal when combined with other personal information about the individual or what risks of harm the disclosure of the

information present to the individual. See also Personal Information above. The Managers, Information Access and Privacy or the Office of General Counsel can advise on the sensitivity of the Personal Information in the context of a specific University Initiative.

18. **The University**: Kwantlen Polytechnic University ("KPU")
19. **The University Executive:** The University's Polytechnic University Executive ("PUE")
20. **University Employee:** a party employed by the University (under FIPPA, the definition of "Employee" includes a Service Provider or volunteer); a non-employee Board member; and a party formerly employed by the University.
21. **University Initiative:** In the context of this Privacy Policy and Procedure, a University Initiative includes any activity or commitment undertaken by a University Employee in the performance of their duties on behalf of the University that involves collection or processing of Personal Information. It may be, among other things, a program, service, or activity of the University, including the use or purchase of a technological solution or software for University activities (irrespective of the dollar value of the initiative).

B. PROCEDURES

1. Collection and Processing of Personal Information
    a. Collection: There are limited authorized purposes for collecting Personal Information under FIPPA. The most common purpose authorizing the University to collect Personal Information under FIPPA is if "the information relates directly to and is necessary for a program or activity" of the University (s. 26(c)). Before collecting an individual's Personal Information, University Employees must consider whether doing so meets these criteria or is otherwise authorized under FIPPA. The University will not collect more Personal Information than is necessary. Personal Information must be collected directly from the individual the information is about unless otherwise authorized under FIPPA. When personal information is collected, individuals must be advised of the authority for collection, purpose for collection, and the contact information of a University Employee who can answer questions regarding the collection, typically a member of the business unit or faculty collecting the information.
    b. Use: Personal Information collected may be used only for the purposes it was originally collected or for a use consistent with that purpose as defined in FIPPA. If University Employees want to use the Personal Information for a secondary purpose, prior written consent from the individual is required in accordance with FIPPA.
    c. Access or Disclosure:
        i. University Employees have the ability to access or disclose a wide range of Personal Information while employed at the University. Before a University Employee accesses an individual's Personal Information or discloses it to another University Employee, the University Employee must be cognizant of whether the access or disclosure is authorized. Except as otherwise authorized under FIPPA, access to or disclosure of Personal Information is authorized only on a "need-to-know" basis, i.e. if it is necessary for the performance of the duties of the University Employee.
        ii. Before a University Employee provides access to or discloses an individual's Personal Information outside of the University, University Employees must consider whether the access or disclosure is authorized under FIPPA.

iii. Access to and disclosure of Personal Information must be done by the most secure means and methods available for the protection of the Personal Information, unless otherwise authorized by Privacy Guidelines, Privacy Advice or Guidance.
iv. Access and disclosure provisions in this section also apply to third party Personal Information.

d. Storage: Personal Information may be stored only in secure, University provisioned or approved storage locations. The University may permit storage of Personal Information outside Canada only in accordance with FIPPA, this Procedure, and KPU Privacy Advice, Guidance, and Guidelines.
e. Retention: Personal Information in the custody or control of the University used to make a decision that directly affects an individual must be retained, under FIPPA, for at least one year after being used for that purpose. The University will not retain unnecessary Personal Information nor retain Personal Information longer than is necessary under FIPPA, other legislation, mandated professional requirements, or for legitimate operational purposes.
f. Protection: Personal Information in any form must be protected against such risks as unauthorized collection, use, access, disclosure or disposal.
g. Disposal: Disposal of Personal Information must be done by secure methods (which render the information irretrievable) and in accordance with the University's prevailing records retention policies and procedures.

2. Requests to Update or Correct Personal Information
    a. Updating Personal Information: Routine requests for updates to Personal Information in the custody or control of the University (for example, change of home address or legal name) can be directed to the Office of the University Registrar (for students) and Human Resources (for University Employees).
    b. Correcting Personal Information: Individuals may submit requests to correct their Personal Information directly to the Office of the University Registrar (for students) or Human Resources (for University Employees). Additionally, individuals may make a request under FIPPA that errors or omissions in their Personal Information held by the University be corrected.

3. Access to Own Personal Information
    a. Individuals (including students) can make requests for access to their own Personal Information by contacting the relevant department directly.
    b. Where the records requested only contain Personal Information about the requesting individual, the records may be released to that individual. If the records contain Personal Information about a third party or Confidential Information (as defined in IM2 Freedom of Information Policy), the University Employee shall immediately advise the Manager, Information Access and Privacy or the Office of General Counsel prior to taking any steps regarding the request.
    c. Additionally, access to information requests may be made under FIPPA as set out under Policy IM2 Freedom of Information Policy and Procedure.
    d. The University has the right to verify the identity of individuals making requests for their Personal Information prior to disclosing it. Verification processes may vary depending on the unit holding the records but processes must be documented to ensure consistent application and shall not result in collection of Personal Information (i.e. do not make a copy of requester identification).

4. Requests for Personal Information from Third Parties
    a. Parties outside of the University requesting that the University disclose or grant them access to another person's Personal Information must provide the University with proof that they are authorized to receive it.
    b. FIPPA sets out various authorizations for disclosure of Personal Information, which include by written consent or authorization from the individual the Personal Information is about. The University has the right to confirm the veracity and adequacy of the consent or authorization as appropriate in the circumstances and require that the consent or authorization include certain content to ensure compliance with FIPPA before proceeding.
    c. If a University Employee receives a request from a third party for Personal Information of another person and the employee is not sure if providing the information is authorized under FIPPA, the employee shall seek advice from the Manager, Information Access and Privacy or the Office of General Counsel prior to disclosing the Personal Information.

5. Privacy Breaches: Most Privacy Breaches at KPU occur internally and accidentally. Immediate action is required in order to contain Privacy Breaches, mitigate potential harms, and comply with privacy obligations under FIPPA.
    a. A University Employee that becomes aware of an actual or suspected Privacy Breach must immediately report it to the Manager, Information Access and Privacy at privacy@kpu.ca.
    b. A University Employee that becomes aware of an actual or suspected Privacy Breach involving KPU IT resources, must report the Privacy Breach simultaneously to the Manager, Information Access and Privacy at privacy@kpu.ca and the Director, Information Security at infosec@kpu.ca, who may immediately take containment measures.
    c. Upon being notified of an actual or suspected Privacy Breach, the Manager, Information Access and Privacy or designate will initiate and coordinate the Privacy Breach Protocol to contain and investigate the breach as quickly as possible.
    d. University Employees involved in reporting, investigating, or addressing a Privacy Breach must provide prompt and full support to the Manager, Information Access and Privacy in respect of the breach.
    e. As Privacy Breaches involve Personal Information and can pose risks of potential harms to affected parties and the University, University Employees must not discuss or share information about a Privacy Breach beyond what is necessary to address the breach. Any internal or external communications in respect of Privacy Breaches will be coordinated by the Manager, Information Access and Privacy or designate.

6. Privacy Incidents
    a. Where a University Employee becomes aware of a Privacy Incident, the employee should report it to their supervisor/manager.
    b. Upon receiving a report in accordance with (a) above, the supervisor/manager must determine whether or not a Privacy Breach has resulted or could result and take appropriate steps to address the incident.

7. Privacy Complaints

a. Privacy complaints will be administered under Policy AD2 Complaints about Instruction, Services, Employees or University.
b. Complainants who are unsatisfied with how the University addresses their privacy complaint may file a complaint with the Office of the Information and Privacy Commissioner for BC ("OIPC") in accordance with OIPC procedures.

8. Privacy by Design and Privacy in Practice:
    a. The University will consider privacy in the planning and implementation of University Initiatives and in relationships within and outside the University by creating or adopting systems, processes, tools, and practices that acknowledge privacy as a key factor.
    b. Further to (a) above, University Employees will be cognizant of how their business practices, daily activities, and interactions impact privacy and will conduct these in ways that protect privacy.

9. Privacy Impact Assessment ("PIA"): under FIPPA, the University must conduct a PIA for University Initiatives and must do so in accordance with FIPPA.
    a. In alignment with Privacy by Design principles, prior to committing to a new, or renewing a current, University Initiative a University Employee undertaking the initiative must ensure that the initiative receives a PIA in accordance with FIPPA, this Procedure, and prevailing University policies and procedures and KPU Privacy Advice, Guidance, and Guidelines. Committing means, for example, executing an agreement/contract, disbursing funds, finalizing the design or process of an activity or program, marketing an activity or program.
    b. Prior to making significant modifications to an existing University Initiative, including a change to the location in which Sensitive Personal Information is stored, a University Employee undertaking the initiative must ensure that the initiative receives a PIA in accordance with FIPPA, prevailing University policies and procedures, and KPU Privacy Advice, Guidance, and Guidelines.
    c. Where a University Initiative involves disclosure of Personal Information to a Third Party (i.e. including but not limited to a vendor, supplier, contractor, consultant, University partner), a PIA must be completed prior to entering into a contract or agreement with the Third Party and before Personal Information is disclosed to or collected by the Third Party. For clarity, a PIA is required:
        i. Whether or not a contract or agreement applies to the University Initiative.
        ii. Irrespective of the dollar value of a contract or agreement related to the University Initiative, including a zero dollar value.
        iii. Whether the University discloses the Personal Information or an individual whose Personal Information it is provides the Personal Information to the Third Party pursuant to the University Initiative.
    d. The University Employee requesting the PIA is responsible for ensuring all information required to conduct the PIA is supplied to the Manager, Information Access and Privacy or designate and that planning for the University Initiative includes time for the PIA to be completed prior to implementation of the initiative.
    e. If a PIA is required in accordance with this section 9, the University Employee undertaking the University Initiative must be accountable for and actively involved in its completion.
    f. PIAs must be reviewed and approved by the appropriate signatories in accordance with FIPPA, prevailing University policies and procedures, and KPU Privacy Guidance or Guidelines before the new/renewed initiative or modification to the existing initiative is implemented.

g. PIAs may result in Privacy Guidance or Guidelines being provided to the University Employee requesting the PIA. The University Employee requesting the PIA is responsible to ensure the Privacy Guidance or Guidelines are shared as necessary (within the University) and to consider the Privacy Guidance or Guidelines in related decision-making and processes.

10. Privacy Risk: Privacy risk exists whenever Personal Information is collected or processed. As the University and University Employees have privacy obligations under FIPPA:
    a. The University and University Employees will identify and take reasonable steps to mitigate privacy risks associated with the collection or processing of Personal Information for University Initiatives in accordance with FIPPA, University policies and procedures, and KPU Privacy Advice, Guidance, and Guidelines.
    b. Reasonable steps to mitigate privacy risks include considering physical, technical, and administrative safeguards for the protection of Personal Information such as the following examples:
        i. Physical: Ensure that Personal Information is kept in locked cabinets and offices, accessible only to authorized individuals; adopt "clean desk" and other privacy-protective work habits.
        ii. Technical: Use only University provisioned or approved products or services; ensure that access to Personal Information is restricted through measures such as role-based access controls, strong passwords, locking computers when away from desk.
        iii. Administrative: Promote and support compliance with FIPPA and University policies, procedures and guidelines relative to the protection of privacy. Establish business practices and processes for proper collection and management of Personal Information and ensure these are documented and followed. Ensure employees are trained on and able to comply with their obligations under FIPPA; related University policies and procedures; and KPU Privacy Advice, Guidance, and Guidelines. Ensure contracts/agreements with Third Parties adequately address the parties' FIPPA obligations.
    c. Privacy risk decisions associated with creating, modifying, or implementing University Initiatives that involve collection or processing of Personal Information, including using Third Party products or services, are made by the relevant University Employee approving the initiative in accordance with FIPPA; prevailing, related University policies and procedures; and KPU Privacy Advice, Guidance, and Guidelines.
    d. Privacy risk decisions must demonstrate consideration of the impact on individuals whose Personal Information is involved and the impact on the University (i.e. potential privacy breaches, non-compliance with FIPPA, reputational risk).

11. Audio or Video Recording, Capture, or Transmission of Personal Information: Audio or video recording, capture (i.e. the taking of screenshots or photos), or transmission (i.e. live streaming) of Personal Information could occur in multiple contexts at the University (i.e. meetings, instructional activities, conversations) and may be subject to obligations and requirements under FIPPA.

    a. Subject to s.1(a), audio or video recording or capture of Personal Information may be considered Collection of Personal Information and create Records under FIPPA.

b. The University will create Guidelines and Protocols for audio or video recording, capture, or transmission of Personal Information for administrative, teaching, and other University activities in order to comply with FIPPA.
c. If a University Employee identifies a need for audio or video recording, capture, or transmission of Personal Information that is not addressed in prevailing Guidelines and Protocols, the University Employee shall seek Guidance from the Manager, Information Access and Privacy or the Office of General Counsel to ensure the proposed recording, capture, or transmission of Personal Information is authorized under FIPPA and this Privacy Policy.
d. Unless otherwise set out in Guidelines, Protocols, or Guidance (in accordance with the above), audio or video recording, capture, or transmission involving Personal Information of any party requires the prior written consent of the individual(s) whose Personal Information is involved as well as other parties to the conversation or meeting.
e. Further to s.11(d), prior written consent shall be obtained in accordance with FIPPA.
f. Audio or video recordings or captures of Personal Information will be used in University proceedings only when authorized by law and in accordance with this Privacy Policy and Procedure.
g. Where audio or video recording or capture of Personal Information is authorized or permitted in accordance with FIPPA and the foregoing, FIPPA provisions pertaining to Records in the custody or control of the University apply. These provisions include use, access, and disclosure limitations and requirements; access requests (i.e. "FOI requests"); privacy protection; and proper storage, retention, and disposal requirements, as outlined in s.1 (a – g) above.

12. Privacy Awareness and Training
    a. University Employees are required to be aware of privacy issues in general and privacy implications specific to their work.
    b. Managers will ensure that the privacy training needs for different functions within their units are identified and the training is provided to University Employees.
    c. All University Employees must complete privacy training deemed necessary by the University.

13. Privacy Resources
    a. KPU Privacy Guidelines and Protocols may be found at the Office of General Counsel Sharepoint site and may be amended from time to time. University Employees are required to stay current with the Guidelines and Protocols as they pertain to the University Employees' work.
    a. University Employees who are uncertain about their privacy obligations or have work-related privacy concerns, should discuss these with their managers who, if necessary, will consult with the Manager, Information Access and Privacy or designate or Office of General Counsel.
    b. Questions or concerns related to the protection of Personal Information or privacy may be submitted to privacy@kpu.ca.

C. RELATED POLICY

Refer to Policy *IM8 Privacy Policy*