POLICY REGARDING THE PROTECTION OF PERSONAL INFORMATION AND ACCESS TO INFORMATION

Effective Date: September 19, 2023

Approval Authority: Secretary-General

Supersedes /Amends: January 12, 2010

Policy Number: SG-9

SCOPE

This Policy applies to all members of the Concordia University (the "University") community and with regard to all Personal Information (as defined below) held by the University.

PURPOSE

The purpose of this Policy is to inform members of the University of their obligations related to the protection of Personal Information that is collected and held by the University.

This Policy:

a) sets out the principles governing the protection of Personal Information throughout its life cycle and the exercise of the rights of individuals;

b) defines the roles and responsibilities of the various stakeholders in relation to the protection of Personal Information;

c) describes the rights of those wishing to access documents that are held by the University and sets out the governing principles; and

d) complies with the *Act respecting Access to documents held by public bodies and the Protection of personal information, chapter A- 2.1* (the "Act"), which establishes the legal framework for the protection of Personal Information held by public bodies, as well as the rights regarding access to information.

DEFINITIONS

For the purposes of this Policy, the following definitions shall apply:

"Commission" means the *Commission d'accès à l'information du Québec*.

"Committee" means the privacy Committee, as set out in this Policy, responsible for supporting the University in carrying out its responsibilities and obligations under the Act.

"Individual(s)" means the person to whom the Personal Information relates.

"Personal Information" means any information (whether it is held in paper, electronic or any other medium) about an individual, which allows an individual to be directly or indirectly identified, including Sensitive Personal Information (as defined below).

"PIA" means a privacy impact assessment performed in accordance with the requirements of the Act.

"Privacy Ambassador" means designated individuals, identified in units throughout the University community, who are trained to provide awareness and to assist the unit personnel notably in: best privacy practices, responding to Privacy Incidents (as defined below), and other compliance processes required to protect Personal Information.

"Privacy Incident(s)" means any unauthorized access to, use of, or disclosure of Personal Information, or any loss or breach of the security of such information.

"Privacy Incident Register" means the register constituted to record Privacy Incidents.

"Privacy Incident Response Plan" means the University's procedure for responding to Privacy Incidents.

"Privacy Notice" means a document(s), available on the University websites, which can be consulted by individuals, including students, staff and faculty, which sets out the way the University collects and uses Personal Information.

"Privacy Officer" means the individual designated to be responsible for the application of the Act within the University.

"Sensitive Personal Information" means any Personal Information which, due to its highly personal nature, and/or the context of its use or communication, requires a higher level of confidentiality.

POLICY

Collection

1. The University and its personnel collect Personal Information that is necessary for the fulfillment of its mission and activities.

2. Personal Information is collected from an Individual based on clear, free and informed consent given for specific purposes. Such consent is valid for the time necessary to fulfill the purposes for which it was requested.

3. At the time of collection and subsequently upon request, through a Privacy Notice or otherwise, the University informs the Individuals concerned of the purposes and methods of collecting and processing their Personal Information as well as their rights with respect to such information.

Use

4. Personal Information concerning past, current or future members of the University community must only be used for the purposes for which the information was collected.

5. The University may, with the consent of the Individual or if permitted by the Act, use Personal Information for other purposes.

6. The University manages the access rights of members of the University community to Personal Information so that only those members who require access to Personal Information in the course of their duties have such access.

Communication

7. Subject to the exceptions permitted in the Act, the University may not disclose Personal Information without the consent of the concerned Individual. Consent must be expressly given when Sensitive Personal Information is involved.

8. When Personal Information is communicated to a third party for, notably, the following reasons:

   a) as part of a service agreement, including a technology tool that is supported on a cloud, or

   b) for the performance of a mandate, or

   c) in collaboration with an external entity

   the University must, when required by the Act, conduct a PIA and enter into an agreement with the relevant service provider or entity. Such agreement must contain the obligations imposed by the Act and as set out, notably, in the University's Privacy Addendum, available on the University's websites.

Privacy Impact Assessments (PIA)

9. The University shall conduct a PIA in, notably, the following situations:

   a) for any project to acquire, develop or overhaul an information system or electronic service delivery system involving the collection, use, release, keeping or destruction of the Personal Information of individuals; and

   b) where it plans to communicate Personal Information without consent to a person or body that wishes to use the information for study, research or statistical purposes.

10. When conducting a PIA, the University considers the sensitivity of the information being collected, shared or stored, the purpose of its use, its quantity, its distribution, including the medium of distribution, as well as the adequacy of the measures proposed to protect Personal Information.

Research Activities and Access to Personal Information

11. Researchers may request to access Personal Information held by the University for research purposes. Such requests must be submitted to the Privacy Officer.

12. When the PIA concludes that Personal Information may be disclosed for this purpose, the University shall enter into an agreement with the researchers containing the required legal obligations.

Registers

13. The University records, in the appropriate registers, instances where Personal Information is shared with third parties, notably in the following cases:

    a) when the University communicates Personal Information necessary for the application of a collective agreement, decree, order, directive or regulation that establishes working conditions;

    b) when the University communicates Personal Information to an agent or service provider as part of a mandate or service agreement;

    c) when the University communicates Personal Information for study, research or statistical purposes;

    d) when Personal Information is used within the University, without the prior consent of the concerned Individual, for a purpose other than the purpose stated at the time of collection but where such use is compatible with the purposes for which it was collected and is clearly for the benefit of the concerned Individual, or is necessary for the application of a law in Quebec;

    e) when disclosure of Personal Information is made to a person or organization that may reduce the risk of serious harm associated with a Privacy Incident; and

    f) Privacy Incidents.

Retention

14. The University takes all reasonable steps to establish that the Personal Information it holds is current, accurate and complete for the purposes for which it is collected or used.

15. The University retains Personal Information for as long as required to conduct its activities, subject to time limits set out in the Records Classification and Retention Plan.

Security Measures

16. The University implements reasonable security measures aimed at protecting the confidentiality, integrity and availability of Personal Information collected, used, disclosed, retained or destroyed. These measures take into account, among other things, the sensitivity of the Personal Information, the purpose for which it is collected, its quantity, its location and its medium.

Privacy Incidents

17. Privacy Incidents shall be addressed in accordance with the law and with the University's Privacy Incident Response Plan.

18. Privacy Incidents must be reported to the Privacy Officer and recorded in the Privacy Incident Register.

19. If it is determined that the Privacy Incident presents a risk of serious harm to the concerned Individuals, the University will notify the concerned Commission.

Individuals Rights

20. Any Individual whose Personal Information is held by the University has the right to:

    a) access their Personal Information held by the University and to obtain a copy of it; and

    b) seek the rectification of any incomplete or inaccurate Personal Information held by the University.

21. While the right of access can be exercised at any time, access to documents containing this information is subject to certain exceptions identified in the Act.

22. Documents containing Personal Information may be consulted on site or can otherwise be accessed with or without paying a fee. Where applicable, information regarding the

requirement to pay a fee is made available prior to processing requests for access to documents.

23. Requests by Individuals for access to their Personal Information may be made verbally or in writing. Verbal requests will be handled informally and may not receive a written reply.

24. Requests by Individuals for access to their Sensitive Personal Information must be made in writing and will receive a written reply.

25. Requests by third parties for access to Personal Information must be directed to the Privacy Officer.

26. Requests for access to Personal Information must be specific enough to allow the Privacy Officer to locate the Personal Information. The right of access applies only to existing Personal Information.

27. University personnel who wish to access their employment-related documents shall access them directly via Carrefour or by making a request directly to Human Resources.

28. Students who wish to access documents related to their enrolment, shall access them directly via the Student Information System (SIS) or by making a request to the relevant unit that provides services to students, including the Birks Student Service Centre, the Student Accounts Office, Counselling and Psychological Services, the Access Centre for Students with Disabilities, or the relevant academic departments.

Exceptions to the Application of the Act Regarding the Release of Personal Information

29. The University may refuse to release information about an Individual when it is contained in an opinion or recommendation when a final decision has not been made on the matter that is the object of the opinion or recommendation.

30. In cases where a document contains Personal Information that would identify a third person, or where another legal exception would apply, the document may not be released, or the document may be released with this information redacted.

31. The right to access does not extend to personal notes written on a document or to drafts, preliminary notes, or outlines of documents.

32. The University may release Personal Information without the consent of the concerned Individual in certain situations, including:

    a) when the University has contracted with a third party to provide a service. Subject to specific protections, regulations and processes, the University may share Personal Information with third parties for the purposes of the services being rendered;

    b) if, by law, the information in question is public, including for example, an employees' contact information at work, including work email address;

    c) in accordance with the *Policy on the Emergency Release of Personal Information* (SG-5);

    d) to an authorized person of the Commission; or

    e) pursuant to a law, court order or subpoena.

Destruction and Anonymization

33. Once the purposes for which Personal Information was collected have been fulfilled, the information will be destroyed or anonymized, subject to the time limits set out in the University's retention schedule, records management policies and any other legal requirements.

Committee

34. As part of its mandate, the Committee:

    a) supports the University in the exercise of its responsibilities and the performance of its obligations under the Act;

    b) approves the University's governance rules regarding Personal Information published on the University's website; and

c) receives updates about and, as required, is consulted regarding the performance of PIA's for any project to acquire, develop or overhaul an information system or electronic service delivery system involving the collection, use, release, keeping or destruction of Personal Information.

Privacy Officer

35. The person responsible for the application of this Policy and the protection of Personal Information at the University is the Secretary-General, who acts as the Privacy Officer.

36. The Privacy Officer:

a) coordinates and manages the Committee;

b) promotes and oversees compliance with the Act, including acknowledging receipt of access requests, assisting the requestor in clarifying the request and/or explaining the reasons for refusal; and

c) receives and treats complaints related to the protection of Personal Information.

University Personnel

37. Personal Information held by the University is confidential and must always be treated as such. In particular, University personnel shall:

a) access only the Personal Information necessary to perform their duties;

b) use such Personal Information only in the course of their duties;

c) not disclose any Personal Information that comes to their knowledge in the course of their duties unless duly authorized to do so;

d) only keep or integrate Personal Information in the files or records required for the performance of their duties;

e) manage Personal Information in such a way that only authorized personnel have access to it;

f) password protect all access to Personal Information in their possession or to which they have access to;

g) dispose of all waste paper by shredding or via confidential recycling if it contains Personal Information;

h) promptly inform the appropriate Privacy Ambassador, designated Individual(s) or the Privacy Officer of any situation or irregularity that could, in any way, compromise the security, integrity or confidentiality of the Personal Information, including a possible Privacy Incident; and

i) will not, at the end of their employment or contract, retain any Personal Information collected or transmitted in the course of their duties and shall maintain their obligation of confidentiality.

38. Sharing of Personal Information between University personnel and units must be limited to sharing of such information that is strictly necessary to carry out duties or fulfill specific roles and for only the purpose for which the Personal Information was collected.

39. Before creating a document containing Personal Information, University personnel shall consider whether the creation of such a record or document is necessary and required.

40. Appropriate security measures must be taken to protect Personal Information and to prevent unauthorized access to such information.

41. University personnel shall conserve and/or destroy Personal Information in compliance with applicable laws and the University's applicable policies, in particular the *Policy on Records Management and Archives (SG-10)* and the *Policy on Email Management (SG-11)*.

42. From time to time, University personnel who are responsible for administrative or academic units shall verify that appropriate and adequate measures are taken within units with respect to the protection of Personal Information. Such an obligation is also in conformity with the *Information Security Policy (VPS-33)*.

43. University personnel will be offered training sessions and awareness activities conducted by the University regarding the protection of Personal Information.

Changes to this Policy

44. This Policy may be updated periodically to comply with changes to the Act and/or to improve the University's privacy practices.

Policy Responsibility and Review

45. The overall responsibility for implementing and recommending amendments to this Policy is the Secretary-General.