DALHOUSIE UNIVERSITY **Privacy Policy**	*Policy Sponsor:* President	*Approval Date:* December 9, 2022
	Responsible Unit: Privacy Office	*Amendments:*

A. <u>Background & Purpose</u>:

The University respects the privacy of individuals and is committed to promoting a culture of privacy that enables protection of privacy and continuous improvement of privacy practices.

The purpose of this policy is to:

1. Establish a formal privacy management program that supports the development of systems and processes that protect privacy.

2. Ensure that the University complies with all applicable privacy laws governing personal information in its custody or control.

3. Ensure that all individuals working and conducting research within, for or on behalf of the University understand their responsibilities and are accountable for protecting personal information and respecting the privacy rights of individuals, when carrying out their duties.

B. <u>Application</u>:

i. This policy applies to:
    a. Individuals employed by Dalhousie on a permanent, temporary, part-time, or contract basis;
    b. Paid and unpaid researchers, including students;
    c. Service providers contracted to handle personal information in the custody and control of the University;
    d. Volunteers, including Dalhousie's Board of Governors;
    e. All personal information (as defined in Nova Scotia's *Freedom of Information and Protection of Privacy Act (FOIPOP)*) under the custody or control of Dalhousie University:
        i. in all recorded formats, digital or paper and in all storage locations;
        ii. related to staff, faculty, students, alumni, clients, members of the public, and other individuals involved in Dalhousie operations and activities.

ii. This policy does not apply special purpose activities such as non-Dalhousie entities that use or rent space at Dalhousie where the activities that are conducted in those spaces are not conducted for or on behalf of the University.

C. Definitions:

Terms used in this policy are defined in Appendix "A" of this Policy.

D. Policy:

1. Accountability

i. The University is accountable for managing personal information in its custody or under its control in accordance with applicable privacy laws, collective agreements, contracts, this policy and its procedures, and other applicable university policies and procedures.

2. Minimization of Personal Information

i. Collection, use, or disclosure of personal information shall be limited to the minimum amount of personal information necessary to achieve the purposes identified at the time of collection.

3. Collection

i. The University shall collect personal information when:
   a. The information relates directly to and is necessary for an operating program or activity of the University;
   b. The collection is expressly authorized by an enactment of Nova Scotia or Canada; or
   c. The information is collected for the purpose of law enforcement.

ii. The purposes for which personal information is being collected shall be provided to the individual at the time of collection when it is collected directly from the individual

iii. The University will collect personal information directly from the individual the information is about unless there is a reasonable requirement to collect from another source and the indirect collection is permitted under *FOIPOP*.

iv. The University shall obtain either express or implied consent prior to collection of personal information except in limited circumstances under *FOIPOP* where collection, use or disclosure are permitted without an individual's consent.

v. Consent must be specific, knowledgeable, and freely given by the individual in order to be valid.

4. Use

i. Personal information shall only be used:

a. For the purpose for which the information was obtained or compiled or a purpose that has a reasonable and direct connection with the original purpose of collection where the use is necessary for meeting a statutory duty or operating an authorized program or activity of the University;
b. The individual has provided consent, express or implied for the use of the personal information; or
c. For purposes expressly permitted, such as research and archival purposes, or required by law.

5. Disclosure

i. Personal information shall only be disclosed to individuals or organizations outside the University under the following circumstances:

a. The disclosure is for the purpose identified at the time of collection or for a purpose consistent with the original purpose;
b. The individual that the personal information is about has consented to the disclosure; or
c. The disclosure is permitted by this policy and its associated procedures or is expressly permitted or required by law.

ii. Disclosure of the following personal information without consent is permitted:
a. A faculty or staff member's remuneration, where the amount of remuneration is over fifty thousand dollars;
b. The names of individuals who received degrees, the period of registration, the certificate, diploma or degree awarded, and the field of study (in relation to the degree awarded), as well as the individual's hometown and awards/distinctions as indicated in the convocation program;
c. Necessary personal information in emergency situations, if the University believes, in good faith, that knowledge of that information is required to protect the health and safety of the individual or other persons;
d. Personal information required to comply with a court order or subpoena;
e. Personal information that is permitted by law to be disclosed without consent or its disclosure is required by law.

iii. Disclosures of personal information outside of Canada, including storage and access, must be done in compliance with *Personal Information International Disclosure Act PIIDPA*, this policy and the University's Access, Storage and Disclosure of Personal information Outside of Canada Procedure.

6. Dalhousie User Access

i. Access to personal information shall be restricted to those who need to know the information by virtue of their role, as determined by the appropriate representatives of the University.

7. Safeguards

i. The University will ensure reasonable safeguards are in place to protect personal information in its custody, or under its control by making security arrangements to protect against such risks as loss, theft, unauthorized access, collection, use, disclosure, storage or disposal.

8. Accuracy and Correction

i. The University shall make every reasonable effort to ensure that personal information in its custody or under its control is accurate and complete.

ii. Where possible, individuals will be able to correct or update certain categories of personal information, such as contact information, on their own.

iii. For other types of personal information believed to be inaccurate, an individual may request that their personal information be corrected by the unit holding the information.

iv. If the unit is unable to make the correction for any reason, or if the individual wishes to make a formal request for correction under the *FOIPOP* act, the request must be made to the Privacy Officer.

9. Retention and Disposal

i. Personal information shall be retained for only as long as is necessary to achieve the purposes for which it was collected, or for legal or other legitimate business purposes, in accordance with this policy, the University's Records Management Policy and the University's record retention schedule.

ii. Personal information used to make a decision that directly affects an individual must be retained for a minimum of one (1) year from the date of the decision in accordance with *FOIPOP*.

iii. Destruction must be secure and take into account the context and sensitivity of the personal information.

10. Access to Information

i. The public has a right to access records, including the right to access records containing personal information about themselves, in the custody or under the control of the University, and subject to specific and limited exceptions under *FOIPOP.*

ii. Formal requests for access to information under *FOIPOP* must be processed in accordance with the University's Access to and Correction of Personal Information Procedure.

iii. The University may provide an individual with access to records containing their personal information without a formal request under *FOIPOP* where those records are routinely made available to individuals (e.g. student transcripts).

11. Providing Health Care, Collecting Health Card Numbers and the Personal Health Information Act

i. The collection, use, and disclosure of the Provincial health card number is regulated by Nova Scotia's *Personal Health Information Act* (*PHIA*) and its regulations.

ii. The University shall only collect and use an individual's health card number for the purposes of facilitating the provision of health services insured by the province of Nova Scotia or for the purpose of REB approved research where a treatment protocol is administered to participants. For example, a University run daycare or camp may request that a parent provide their child's health card number to use in the event of a health emergency, but the University cannot collect and use health card numbers as a means of identification.

iii. Where personal health information is collected, used or disclosed by the University for the purpose of providing health care to individuals, *PHIA* and its regulations apply to the management and protection of personal health information.

12. Research and Innovation

i. Access to personal information in the custody or under the control of the University for the purposes of research may be allowed with the approval of the appropriate Dalhousie Research Ethics Board (REB) and under the conditions specified in s. 29 of *FOIPOP* and s.19B of the *FOIPOP* regulations.

ii. Dalhousie's REB is responsible for matters related to Indigenous research conduct. Under this policy, Indigenous research (as defined by the tri-council), shall follow guidance from the Tri-Council Policy Statement (TCPS2) Privacy and Confidentiality Articles 9.16; Ownership, Control, Access and Possession (OCAP); and guidance from Indigenous and Métis communities, where appropriate.

13. Access, Storage and Disclosure outside of Canada

i. The University shall ensure that personal information in its custody or under its control will be stored only in Canada, accessed only from Canada, and disclosed only within Canada, unless certain conditions exist, in accordance with Nova Scotia's *Personal Information International Disclosure Act (PIIDPA)* and the University's Access Storage and Disclosure of Personal Information Outside of Canada Procedure. These requirements also apply to University service providers contracted to handle personal information in the custody or under the control of the University.

ii. Personal information may be transported temporarily outside Canada for access purposes only in accordance with the University's Access Storage and Disclosure of Personal Information Outside of Canada Procedure.

iii. Any requests for disclosure of personal information in the custody or under the control of the University by authorities or organizations outside of Canada, such as a foreign court, state agency or law enforcement entity, shall be directed to the University's Legal Counsel Office.

14. Privacy Impact Assessments

i. A risk-based Privacy Impact Assessment (PIA) must be conducted for all new Dalhousie University systems, projects, programs, or activities and for substantially modified systems or activities that collect, use, store and disclose personal information. The nature and extent of the assessment will be based on risk.

ii. PIAs must be reviewed, completed, and approved in accordance with this policy's Privacy Impact Assessment Procedure before a new system, project, program or activity can be tested and/ or implemented and before substantial modifications to an existing system can be implemented.

15. Privacy Incident and Breach Management

i. All known or suspected privacy breaches must be handled in accordance with this policy and the University's Privacy Incident and Breach Protocol.

ii. Records related to privacy breaches shall be retained, in a separate file, for two years from the date the University closes the privacy breach investigation.

16. Privacy Complaints/Challenging compliance

i. Individuals are entitled to make a formal privacy complaint to the University Privacy Officer regarding Dalhousie University's compliance with this policy, the Privacy Complaint Procedure, associated procedures and applicable privacy laws.

ii. In cases where a privacy complaint relates to the privacy provisions of *FOIPOP,* individuals have the right to ask the Office of the Information and Privacy Commissioner of Nova Scotia for a review of their privacy complaint once the University's internal privacy complaint process is completed.

17. Non-compliance with policies and procedures

i. Non-compliance with this policy, its associated procedures, and applicable privacy laws may be subject to penalties under University regulations, collective agreements, contracts and provincial and federal law.

E. Administrative Structure:

1. *Authority:* This policy falls under the authority of the Board of Governors.

2. *Policy Review:* This policy will be reviewed every five years or earlier if the policy is no longer compliant with applicable laws or if a review is deemed necessary by the Board of Governors.

3. *Heads of Academic and Administrative Units:*
   The head of an academic or administrative unit is responsible for:
   i. familiarizing themselves with the requirements of this policy, its procedures, and applicable privacy laws and communicating requirements to staff and faculty n their units;
   ii. making reasonable efforts to ensure that management of personal information in their units meets the requirements of this policy, its procedures, and applicable privacy laws;
   iii. reporting any privacy incidents or breaches, in accordance with the University's Privacy Breach Protocol; and
   iv. conducting risk-based privacy assessments under s 14 of this policy.

4. *Staff, Faculty, Students and Volunteers:*
   Staff, Faculty, Students and Volunteers are responsible for:
   i. taking reasonable steps to protect all personal information entrusted to them in accordance with this policy, its procedures, and applicable privacy laws;
   ii. actively participating in privacy training and familiarizing themselves with this policy, its procedures, and applicable privacy laws; and
   iii. reporting privacy incidents or breaches in accordance with this policy and its procedures.

5. *Third Parties:*
   i. Third-party service providers whose work on behalf of the University involves the collection, access, use or disclosure of Personal Information must abide by this policy, its procedures and all applicable privacy laws in its handling of personal information.
   ii. The University shall ensure that contractual means are in place to protect personal information collected, accessed, used, disclosed or retained by third party service providers as part of their work for the University.

6. *Privacy Officer*
   i. The Privacy Officer is responsible for promoting, monitoring, and reporting on compliance with *FOIPOP* and with this policy. The Privacy Officer's responsibilities include:
      a. Providing privacy advice and consultation
      b. Supporting training and relevant information exchange;
      c. Providing ongoing assessment of privacy risks;
      d. Responding to and providing advice regarding privacy incidents and breaches; and

e. Responding to privacy complaints.

7. *Annual Reporting:* At the end of each academic year, an annual privacy report will be delivered to the Board of Governors which will include:
   i. The number of access to information applications processed under *FOIPOP* with the following details:
      a. representation of the applications by request type (e.g., business, political party, third-party representative, private individual/public, public interest group);
      b. total received;
      c. total withdrawn/abandoned;
      d. requests transferred out;
      e. access decisions (e.g., access granted in full, part, no record/not in custody or under the control of the University);
      f. decision response time (e.g., within 30 days, withing 60 days, 60 days or more); and
      g. Fees collected (e.g., application fees and processing fees).
   ii. Office of Information & Privacy Commissioner (OIPC) Reviews – number of requests for reviews, resolved without formal review, formal reviews.
   iii. Number of PIAs completed with the following details:
      a. A representation of the types of tools and processes where PIAs were completed;
      b. Number PIAs that went to Information Governance Steering Committee (IGSC) for approval; and
      c. Summary of general risk and mitigations.
   iv. Number of privacy complaints, incidents or breaches including a summary of occurrence, response, and outcome.

F. Procedures:

1. General Counsel may approve procedures that support the management and protection of personal information pursuant to this policy. General Counsel shall determine in advance what consultation, if any, is required before deciding whether to approve a given procedure.

G. Relevant Legislation:

Freedom of Information and Protection of Privacy
Personal Information International Disclosure Protection Act
Personal Health Information Act

H. Related Policies and Procedures:
Management of Personal Information Procedure
Privacy Incident and Breach Protocol

Privacy Complaint Procedure
Access, Storage and Disclosure of Personal Information Outside of Canada Procedure
Privacy Impact Assessment Procedure
Access to and Correction of Personal Information Procedure
Research Ethics Policy (in development)
Indigenous Research Policy (in development)

Appendix "A" - Definitions

In this policy:

1. "**Access**" means the ability to view or obtain information.

2. "**Access to information**" means the right of the public to view or obtain a copy of records, and the right of individuals to view or receive a copy of records containing their own personal information, in the custody or under the control of the University, subject to specific legal exemptions.

3. "**Collection**" means the act of gathering, acquiring, or obtaining personal information by any means from any source, except it does not include the sharing of personal information between authorized Dalhousie faculty, staff, volunteers and service providers.

4. "**Confidentiality**" means the obligation of an individual or an organization to protect personal information entrusted to it and not misuse or wrongfully disclose it.

5. "**Disclosure**" means making available or releasing personal information by any means to any individual or entity, except it does not include the sharing of personal information between authorized Dalhousie faculty, staff, volunteers and service providers.

6. "**Express consent**" means an individual's permission for the collection, use and/or disclosure of their personal information is explicitly and directly given. Express consent may be written or verbal.

7. "**Health care**" means an observation, examination, assessment, care, service or procedure in relation to an individual that is carried out, provided or undertaken for one or more of the following health related purposes:
    i. the diagnosis, treatment or maintenance of an individual's physical or mental condition,
    ii. the prevention of disease or injury,
    iii. the promotion or protection of health,
    iv. palliative care,
    v. the compounding, dispensing or selling of a drug, healthcare aid, device, product, equipment or other item to an individual or for the use of an individual, under a prescription, or
    vi. a program or service designated as a healthcare service under *PHIA*'s regulations.

8. "**Implied consent**" means an individual's permission for the collection, use and disclosure of their personal information can be reasonably inferred from the circumstances, i.e. their actions and other available information.

9. "**In the custody or under the control of the University**" means records or personal information related to the University's mandate and function that the University has some power of direction or command over or are accessible to the University based on customary practice. For example, personal information and records that relate to personal matters and are wholly unrelated to the University's mandate would not be in the University's custody and control, while administrative records connected to the University's mandate would ordinarily be under the University's custody and control.

10. "**Knowledgeable**" means it is reasonable in the circumstances to believe the individual understands what personal information will be collected, how it will be used, and with whom it will be disclosed.

11. "**Personal health information**" means identifying information about an individual (i.e. information that identifies or could reasonably be used to identify an individual either alone or with other information), whether living or deceased, and both in recorded and unrecorded forms, that relates to:
    - The physical or mental health of the individual, including information regarding the health history of the individual's family,
    - The application, assessment, eligibility and provision of health care to the individual, including the identification of a person as the individual's health care provider,
    - Payments or eligibility for healthcare in respect of the individual,
    - The individual's registration information, including their health card number,
    - Identification of the individual's substitute decision maker, or
    - The donation by the individual of any body part or bodily substance, or information derived from the testing or examination of the same.

12. "**Personal information**" means recorded and unrecorded information about an identifiable individual, including, but not limited to:
    - The individual's name, address or telephone number,
    - The individual's age, sex, sexual orientation, marital status or family status,
    - An identifying number, symbol or other particular assigned to the individual
    - The individual's fingerprints, blood type or inheritable characteristics,
    - Information about the individual's healthcare history, including a physical or mental disability,
    - Information about an individual's educational, financial, criminal or employment history,
    - Anyone else's opinions about the individual, and
    - The individual's personal views or opinions, except if they are about someone else.

13. "**Privacy**" means an individual's right to control how, when and to what extent their personal information is collected, used and disclosed.

14. "**Privacy breach**" means an event that results in unauthorized access to or the unauthorized collection, use, disclosure, or disposal of personal information or personal health information in

the custody or under the control of the University. Such activity is unauthorized if it occurs in contravention of applicable privacy laws, this policy and its associated procedures, collective agreements, and contracts. Privacy breaches may be intentional or unintentional.

15. "**Privacy complaint**" means a complaint from an individual who believes that their personal information, in the custody or under the control of the University, has been handled in a manner contrary to the University's privacy obligations under applicable privacy laws, this policy and its procedures.

16. "**Privacy impact assessment**" means a due diligence process in which the University identifies and addresses potential privacy risks to personal information in its custody or under its control that may occur in the course of University operations.

17. "**Privacy laws**" means laws that set out obligations for the University in relation to the privacy of personal information, including, but not limited to:
    - Nova Scotia's *Freedom of Information and Protection of Privacy Act (FOIPOP)*,
    - Nova Scotia's *Personal Information International Disclosure Protection Act (PIIDPA)*,
    - Nova Scotia's *Privacy Review Officer Act (PROA)*,
    - Nova Scotia's *Personal Health Information Act (PHIA)*, or
    - Canada's *Personal Information Protection and Electronic Documents Act (PIPEDA)*.

18. "**Privacy management program**" means a formal comprehensive framework for managing and protecting the privacy of personal information in the custody or under the control of the University. Elements of the framework include governance and reporting mechanisms, program controls such as policies and training requirements, and continuous improvement processes.

19. "**Research**" means "an undertaking intended to extend knowledge through a disciplined inquiry or systematic investigation."

20. "**Record**" means the following, as set out in s. 3(1) (k) of *FOIPOP*:

    "record" includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other things on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records."

21. "**Security**" means the tools and techniques used to protect the confidentiality, availability and integrity of personal information.

22. "**Service provider**" means a person or organization retained under contract to perform services for the University.

23. "**Significant change**" means a change that would pose new risks to the privacy of personal information.

24. “**Unit**” means an academic or administrative unit within the University.

25. “**University community**” means faculty, staff and students of Dalhousie University and others engaged in activities under the auspices of Dalhousie University.

26. “**Use**” means handling or dealing with personal information in the custody or under the control of the University, including the sharing of personal information between faculty, staff, volunteers and service providers of the University, but does not include collection or disclosure of personal information.