Policy Name: Personal Information Protection
Approving Authority: President

Policy # AD-009
Approval Date: 12/22/2023
Date Last Reviewed: 12/22/2023
Next Review Date: 12/2024

Statement

The Personal Information Protection policy of Beal University Canada ("BUC" or the "University"), underscores the commitment of the University to ensure confidentiality and responsible handling of sensitive data in accordance with applicable laws and industry standards. The Personal Information Protection Policy is approved by the President. The policy will be reviewed annually by the IT Governance Committee.

Purpose

The purpose of the Personal Information Protection policy is to ensure the University maintains compliance with the Personal Information Protection and Electronic Documents Act, hereinafter referred to as "PIPEDA", the Right to Information and Protection of Privacy Act (RTIPPA), and other applicable privacy legislation.

Roles and Responsibilities

This policy applies to:

- All members of the University community involved in the collection, storage, access, use, disclosure, retention or disposition of personal information in the conduct of their BUC functions or activities.
- All members of the University community responsible for managing personal information in their care, custody, or control according to this policy.
- Third parties requiring access to personal information in order to perform a recognized University function or activity who shall be bound by this policy and by the terms of a written information sharing agreement.

All members of the University community are responsible for the implementation of this policy and are responsible to:

- be aware of this policy and all other policies related to the management of personal information;
- respond to individuals exercising their right to access and revise their personal information under Privacy Principle 4, as provided for in the PROCEDURE TO ACCESS AND REVISE PERSONAL INFORMATION Section of this policy;
- work with the Director of IT/Privacy Officer to resolve challenges and appeals as provided for in the PROCEDURE FOR CHALLENGES AND APPEALS Section of this policy;
- assist the individual at the department or unit level to the extent of their knowledge and ability; and
- otherwise act as appropriate to manage personal information in a manner consistent with this policy, the 10 Privacy Principles and applicable privacy legislation.

Members of the University community in supervisory and management roles in addition to the above responsibilities are required to:

- notify new staff of the existence of this policy and any related procedures and their locations;
- revise related guidelines or procedures as required to conform to this policy; and
- assist the Director of IT with the resolution of disputes over decisions that may be unfavourable to applicants or third parties.
- ensure practices and procedures are in place for the management of personal information in their

area(s) of responsibility, which are sufficient to ensure implementation of this policy, the 10 Privacy Principles and compliance with privacy legislation;
- consult with the Director of IT on questions regarding the application and interpretation of this policy;
- inform the Director of IT of disputes encountered in discharging their responsibilities under this policy; and
- ensure that the transfer, disclosure, or retention of personal information to and by persons in a third-party relationship with the University (including contractors and executive members of recognized student organizations) for any reason, is pursuant to specific contractual agreements that preserve the privacy protections of this policy.

The Director of IT, designated by the President, shall in addition to the above responsibilities:
- assist other members of the University community in responding to requests and queries from individuals under this policy, or with respect to the 10 Privacy Principles and applicable privacy legislation;
- receive, and respond to, challenges pursuant to PROCEDURE FOR CHALLENGES AND APPEALS Section of this policy concerning the University's compliance with:
  - this policy;
  - applicable federal and provincial legislation; and
  - any other University policy or procedure related to the management of personal information that does not include its own specific procedure for dealing with compliance;
- otherwise assist other members of the University community, including members who work at off-campus sites, in discharging their responsibilities under this policy.

The Director of IT shall, in addition to the above responsibilities:
- hold overall responsibility for the implementation and application of this policy and may develop and recommend periodic revisions;
- respond to questions of interpretation of policy and legislative requirements; and
- receive and respond to appeals pursuant to PROCEDURE FOR CHALLENGES AND APPEALS Section of this policy.

Definitions

PIPEDA: is the Personal Information Protection and Electronic Documents Act, hereinafter referred to as "PIPEDA" and is a federal law that legislates standards for the management of personal information by organizations engaged in commercial activities. PIPEDA applies to Universities even though the scope of their commercial activities may be limited. PIPEDA holds organizations accountable for personal information in their care, custody or control, and requires that reasonable limits be placed on the collection, storage, access, use, disclosure and retention of personal information. In addition, PIPEDA requires openness with regard to an organization's privacy policies and practices.
- This policy only applies to personal information that the University collects, uses or discloses in the course of commercial activities.
- This policy does not apply to employee and student information collected, used or disclosed in the administration of the University unless and until that information is used or disclosed in the course of a commercial activity.
  - The University will collect, use or disclose personal information in the course of a commercial activity only for purposes that a reasonable person would consider appropriate in the circumstances and to the extent necessary to complete that activity. Given the forgoing, and that the commercial activities will be ones in which

an individual participates voluntarily, and since it is the University's policy not to use or disclose personal information collected in the course of one commercial activity in any other commercial activity, the University believes that the individual's participation in the activity constitutes sufficient consent to collect that information and that express disclosure of the use that will be made of the personal information is not required. Furthermore, since personal information that the University collects other than in the course of a commercial activity will only be used in the course of commercial activities in very limited circumstances that are reasonable given the work of the University, such as to provide services to members of the Alumni, express consent is not required for the University to make use of that information.

RTIPPA is the Right to Information and Protection of Privacy Act ("RTIPPA") and is New Brunswick's access to information and protection of privacy legislation. The provisions of RTIPPA will apply to all management of personal information.

Both PIPEDA and RTIPPA are informed by internationally recognized and accepted fair information principles known as the 10 Privacy Principles. Adoption of the 10 Privacy Principles in all areas of personal information management at BUC will ensure that our legislated obligations are met.

- PERSONAL INFORMATION means recorded information about an identifiable individual in any form. The form or medium in which the information may be recorded includes, for example, images, audio recordings and text whether digital or hard copy.

- MANAGEMENT OF PERSONAL INFORMATION includes all administrative and operational activities carried out by members of the University community, which are connected with the collection, storage, accessing, use, disclosure, retention or disposition of personal information.

- MEMBERS OF THE UNIVERSITY COMMUNITY
  - All employees including but not limited to full-time faculty and librarians, contract academic employees, full and part-time support staff, teaching assistants, graduate students and undergraduate students;
  - All persons holding non-employment appointments including but not limited to adjuncts, stipend instructors, visiting professors and;
  - Any other person who has access to information for the purpose of conducting administrative or operational functions or activities at BUC.

Policy

This policy ensures that the University implements best practices for the management of personal information and protection of privacy through responsible management of information.

This policy is based on and incorporates the 10 Privacy Principles. The 10 Privacy Principles are widely recognized and accepted as the foundation for best information practices. 10 Privacy Principles

They inform PIPEDA, RTIPPA, and other privacy laws in Canada and abroad. By applying the 10 Privacy Principles in all areas of personal information management at BUC, members of the University community may be confident that personal information will be handled appropriately and that legislative requirements will be met.

The principles apply within the university context as set out below:

Principle 1:
ACCOUNTABILITY: This policy is designed to give effect to the principle of accountability by making all members of the University community responsible for managing personal information in accordance with the 10 Privacy Principles.

- This means that all members of the University community are responsible for the management of personal information in their care, custody, or control. This responsibility extends to the disclosure or transfer of personal information for any purpose to persons in a third-party relationship with the University (including contractors and executive members of recognized student organizations).
- The University Director of Compliance, Health, and Safety holds overall responsibility for the implementation and administration of this policy.

Principle 2:
IDENTIFYING PURPOSES: When collecting personal information, members of the University community shall inform the individual of the purpose(s) for which the personal information is being collected. Where personal information is collected through completion of a standard form or application, a statement of the purpose(s) on the form or application is advised.

- When collecting personal information, all members of the University community are expected to be fully aware of and able to explain to individuals the purpose(s) for which the personal information is being collected and how it may be used and disclosed.

Principle 3:
CONSENT: All members of the University community shall obtain consent from the individual when collecting personal information. Consent must be tied to the purpose(s) identified at or before the time of collection in accordance with Privacy Principle 2.

Principle 4:
LIMITING COLLECTION: All members of the University community shall limit the collection of personal information to that which is necessary for the administration and operation of University programs and activities, and is reasonably necessary to accomplish the purpose(s) identified at the time of collection. Individuals shall not be asked for personal information beyond what is reasonably necessary for the identified purpose(s). See also COLLECTION Section.

Principle 5:
LIMITING USE, DISCLOSURE AND RETENTION: All members of the University community who are required to use and disclose personal information in the performance of their BUC duties shall limit use and disclosure of personal information to the minimum amount of information necessary to accomplish the purpose(s) identified at the time of collection. Any new or additional use or disclosure of personal information beyond that will require the identification of the new purpose(s) to the individual and the securing of further consent, except as provided in the Policy. See also RETENTION AND USE AND DISCLOSURE Sections.

- The application of this principle means that access to information is only provided if the individual has given express consent to the disclosure for the specific purpose(s) identified. Members of the University community should have access only to personal information that they need for business purposes.
- The retention of personal information is subject to both legal requirements and University record retention and disposition schedules.

- Special Provision for Serious Health or Safety Concerns: Both federal and provincial privacy legislation authorizes the use and disclosure of personal information in circumstances where serious health and safety concerns exist. If a member of the University community apprehends that a health or safety concern may require the use or disclosure of personal information in a manner that is inconsistent with the privacy principles set out in this policy, the member should consult the Director of IT/Privacy Officer, or appropriate University official immediately.
- Special Provision for Other Exceptions: The RTIPPA permits the disclosure of personal information in other specific circumstances listed in the RTIPPA, including but not limited to compliance with subpoenas or court orders, for the purpose of managing or administering personnel of the University, for the purpose of providing legal advice to the University, or for certain research purposes related to receiving and approving a proposal. A full list can be found in the RTIPPA. If a member of the University community believes disclosure may be required under an exception, the member should consult the Director of IT/Privacy Officer and the exception relied upon should be documented.

Principle 6:

ACCURACY: All members of the University community shall take reasonable measures to ensure that personal information in their care, custody or control is as accurate, complete and current as necessary for the purpose(s) for which it is to be used.

- This means that in each area of responsibility, the manager(s) shall develop procedures not in contradiction with this policy to:
  - allow individuals to access and revise their personal information upon request (to the extent it is permitted and consistent with Principle 4 and PROCEDURE TO ACCESS AND REVISE PERSONAL INFORMATION Section), and
  - periodically review and revise personal information to minimize the possibility that inaccurate or incomplete personal information may be used to make a decision about an individual.

Principle 7:

APPROPRIATE SAFEGUARDS: All members of the University community shall ensure that personal information in their care, custody or control is:

- stored in a manner that prevents unauthorized access or destruction;
- accessed, used and disclosed in a manner that is consistent with the identified purpose(s) and does not extend beyond the intended access, use and disclosure;
- disposed of in a manner that prevents disclosure.

The level of protection will be in proportion and appropriate to the sensitivity of the information and the circumstances of its collection, use, and disclosure.

Principle 8:

OPENNESS: All members of the University community, upon request, shall provide a copy of this policy and, if required, additional information about BUC policies, procedures and practices related to the management of personal information. For purposes of providing the policy and any additional information, referral to an online source is acceptable.

Principle 9:
INDIVIDUAL ACCESS: Individuals are entitled to access and review their personal information which is in the care, custody, or control of any member of the University community and which the Director of IT/Privacy Officer is able to access.

- Subsequent to accessing and reviewing personal information, an individual may request revisions related directly to the accuracy and completeness of the personal information (See Section 4.6).

Principle 10:
PROVIDE RECOURSE: Depending on the context, individuals may have recourse to challenges and appeals concerning their personal information as outlined below.

- Challenges: Individuals are entitled to challenge the University's compliance with:
  - this policy,
  - applicable federal and provincial privacy legislation, and
  - any other University policy or procedure related to the management of personal information that does not include its own specific procedure for dealing with compliance.
- Appeals: Individuals are entitled to appeal:
  - Specific decisions rendered by the Director of IT/Privacy Officer

Related Policies and Documents

Addendum: Procedures on Personal Information

Addendum
Procedures on Personal Information

COLLECTION: Personal information shall be collected by BUC directly from the individual unless:

- another method of collection is authorized by that individual or by an Act of the Legislature or an Act of Parliament of Canada,
- collection of the information directly from the individual could reasonably be expected to cause harm to the individual or to another person,
- collection of the information is in the interest of the individual and time or circumstances do not permit collection directly from the individual,
- collection of the information directly from the individual could reasonably be expected to result in inaccurate information being collected,
- the information is collected for the purpose of existing or anticipated legal proceedings to which BUC is a party,
- the information is collected for use in providing legal advice or legal services to BUC,
- the information is collected for the purpose of:
    - determining the eligibility of an individual to participate in a program of or receive a benefit or service from BUC and is collected in the course of processing an application made by or on behalf of the individual the information is about, or
    - verifying the eligibility of an individual who is participating in a program of or receiving a benefit or service from BUC,
- the information is collected for the purpose of:
    - determining the amount of or collecting a fine, debt or payment owing to BUC, or
    - making a payment,
- the information collected for the purpose of managing or administering personnel of BUC,
- the information is collected for the purpose of auditing, monitoring or evaluating the activities of BUC,
- the information is collected for the purpose of determining suitability for an honour or award, including an honourary degree, scholarship, prize or bursary, or,
- the information is collected for some other substantial reason in the public interest, whether or not it is similar in nature to defined in the COLLECTION section.

RETENTION: Whenever BUC uses personal information about an individual to make a decision that directly affects that individual, Members of the University shall ensure that such information will be retained for a reasonable period of time so that the individual to whom the information relates has a reasonable opportunity to obtain access to it.

USE AND DISCLOSURE: Members of the University community shall limit the use and disclosure of personal information in its custody or under its control to those of its officers, directors, employees or agents who need to know the information to carry out the purpose for which the information was collected or received or to carry out a purpose authorized under the RTIPPA (Right to Information and Protection of Privacy Act).

PROCEDURE TO ACCESS AND REVISE PERSONAL INFORMATION: Consistent with Privacy Principle 4, individuals are entitled to access and revise personal information in the custody or control of any member of the University community in accordance with the following procedures.

ACCESS

- Individuals wishing to review their personal information shall request access to the relevant records through appropriate University procedures or the Director of IT/Privacy Officer.
- Members of the University community in supervisory and management roles are expected to establish procedures and protocols for the review of personal information in their areas.
- Procedures and protocols for review shall be consistent with this policy and applicable privacy legislation. All reviews of personal information shall be in compliance with Privacy Principle 4.

REVISION

Subsequent to reviewing personal information, an individual may request revisions related to the accuracy and completeness of the personal information. Requests for revisions shall include sufficient documentation (e.g. marriage certificate, name change form) for the responsible member of the University community to determine if the requested revisions are appropriate.

The responsible member of the University community, taking into account the request for revisions, shall determine what revisions are appropriate to ensure accuracy and completeness of the personal information. The individual and, as necessary, the University Director of IT/Privacy Officer may be consulted in making this determination.

The responsible member of the University community shall make any revisions as determined in (REVISION Section), within 30 days of receiving the request and at no cost to the individual, and shall respond to the individual in writing providing:

- notification to the individual of the revision; or
- if the decision was made not to revise, a summary of the determination made in (REVISION Section) above and the reasons for this decision; and
- notice of the individual's right to challenge this decision under PROCEDURE FOR CHALLENGES AND APPEALS Section of this policy.

When the responsible member of the University community deems that revisions are not necessary to ensure accuracy or completeness of the personal information, the request for correction shall be added to the record(s) in question.

When personal information is revised, any third party to whom the personal information has been disclosed during the previous year shall be notified, where practicable.

PROCEDURE FOR CHALLENGES AND APPEALS

CHALLENGES: Consistent with CHALLENGING AND APPEALING Section, individuals are entitled to challenge the University's compliance with:

- this policy;
- applicable federal and provincial privacy legislation; and
- any other University policy or procedure related to the management of personal information that does not include its own specific provision for dealing with compliance. This includes challenges of any refusal to provide access and any decision pursuant to a request for revision to personal information under PROCEDURE TO ACCESS AND REVISE PERSONAL INFORMATION Section above.

Individuals who wish to file a challenge may submit in writing a statement outlining the substance of their concern to the Director of IT/Privacy Officer.

The Director of IT/Privacy Officer shall, upon receipt of the challenge:

- investigate the concern in consultation with the individual, and, as appropriate, the responsible member(s) of the University community, and decide what further measures, if any, are to be taken to address the challenge; and,
- provide a written report [email is acceptable] to the individual within 30 days, indicating:
  - what actions were taken to investigate and to process the challenge, and
  - further measures, if any, that have been or will be taken to address the challenge.
- The individual may appeal the Director of IT/Privacy Officer's decision as provided for below.

APPEALS

Consistent with Principle 4, individuals are entitled to appeal:

- specific decisions rendered by the Director of IT/Privacy Officer concerning challenges under PROCEDURE TO ACCESS AND REVISE PERSONAL INFORMATION Section, above.

Individuals who wish to appeal shall submit in writing a statement outlining the substance of the appeal to the Director of IT/Privacy Officer.

- The Director of IT/Privacy Officer, upon receipt of an appeal shall:
  - at a minimum, meet with the individual and with any other member of the University community as the President deems appropriate, or delegate someone to meet; and,
  - issue a written decision within 30 days, providing reasons for the decision [email is acceptable]. This written decision shall be final and not subject to further appeal within the University.
- If an individual is not satisfied with the Director of IT/Privacy Officer's decision concerning the appeal, the individual may contact the Access to Information and Privacy Commissioner (RTIPPA) or the Privacy Commissioner of Canada (PIPEDA) to file a complaint. https://www.priv.gc.ca/en/.