SCHEDULE B

GUIDELINE NO. 8: **Rules of Governance for the Protection of Personal Information**	**APPROVED:** **Directors' Table – JUNE 6, 2023** **(with an effective date of September 22, 2023)**

PREAMBLE

This Guideline constitutes a guide for the rules of governance of John Abbott College (hereinafter the "**College**") with respect to the protection of personal information held by the College, as required by the *Act respecting Access to documents held by public bodies and the Protection of personal information*, CQLR, c. A-2.1 (hereinafter the "**Act**").

This Guideline has been approved by the Committee on Access to Information and the Protection of Personal Information (hereinafter the "**Committee**") and by the College Directors' Table, as indicated in paragraph 19 of this Guideline.

For clarification purposes, the Committee is composed as follows:

- Person responsible for access to documents and the protection of personal information;
- Person responsible for document management;
- Director of Information Technology Services;
- Director of Finance;
- Director of Human Resources;
- Dean of Academic Systems; and
- Any other person whose expertise is required.

This Guideline is published on the College's website as prescribed by the Act (s. 63.3 Act). Should a discrepancy arise between the Act and this Guideline, the Act prevails. For any questions regarding this Guideline, please contact the Director responsible of legal affairs at the College.

1. Definitions

In this Guideline, unless the context requires otherwise, the terms below shall have the following meaning:

- Personal Information:

  Any information about a natural person that directly or indirectly permits the identification of that person, such as, but not limited to: their name, address, telephone number, e-mail address, occupation, social insurance number, health insurance number, date of birth, photograph, and banking information.

  Personal information must be protected regardless of the medium in which it is held and regardless of whether it is in written, graphic, audio, visual, computerized or in any other form.

  It should be noted that some personal information is public by law and is not subject to the rules for the protection of personal information set out in the Act (ss. 55 and 57 Act).

- Consent:

  Consent is an authorization given, by the person to whom the personal information relates, to collect and use their personal information. Consent cannot be presumed. It must be clear, free and informed and be given for specific purposes, in clear and simple language, and for the duration necessary to achieve the purposes for which it was requested.

  In this regard, the consent of a minor under 14 years of age is given by the person having parental authority or by the tutor. The consent of a minor of 14 years of age or over is given by the minor, by the person having parental authority or by the tutor (s. 53.1 Act).

- Minor:

  A person under the age of 18.

- Adult:

  A person of 18 years of age or older or an emancipated person under 18 years of age.

2. Scope

As a public organization, the College collects personal information, including from its students, staff members, suppliers and clients of the various services it offers (dental clinic, sports centre, theatre, etc.). This Guideline applies to any person who, in the execution of their duties, collects, consults, uses, communicates, holds or retains personal information held by the College concerning any natural person.

3. Collection of Personal Information

a. Personal information that may be collected (s. 64 Act)

In order to properly carry out its mission, it is reasonable for the College to collect personal information. To that effect, the College shall only collect personal information that is necessary for the exercise of its rights and powers or the implementation of a program under its management.

The Act also stipulates that the College may collect personal information if it is necessary for the exercise of the rights and powers or for the implementation of a program of a public body with which it cooperates to provide services or to pursue a common mission. In such cases, the collection must be preceded by a privacy impact assessment and be carried out within the framework of a written agreement transmitted to the *Commission d'accès à l'information du Québec*, in accordance with the Act.

The College must undertake measures to ensure that the personal information it collects is adequate, relevant, not excessive and used for limited purposes.

b. Information provided at the time of collection (s. 65 Act)

When collecting personal information, the College must ensure that the person concerned is informed, at or before the time of collection of the following:

i. the name of the public body on whose behalf the information is being collected;
ii. the purposes for which the information is being collected;
iii. the means by which the information is collected;
iv. whether the request is mandatory or optional;
v. the consequences of refusing to reply or consent to the request;
vi. the rights of access and correction provided by law;
vii. the possibility that the personal information may be disclosed outside of Quebec, if applicable.

On request, the person concerned is also informed of the personal information collected from them, the categories of persons within the College who have access to it, the duration of the period of time the information will be kept and the contact information of the person in charge of the protection of personal information.

c. Profiling at the time personal information is collected (s. 65.0.1 Act)

In addition to the above information that must be provided, anyone who collects personal information from the person concerned using technology that includes functions allowing the person concerned to be identified, located or profiled must first inform the individual:

i. of the use of such technology;
ii. of the means available to activate the functions that allow a person to be identified, located or profiled.

Profiling means the collection and use of personal information to assess certain characteristics of a natural person, in particular for the purpose of analyzing that person's work performance, economic situation, health, personal preferences, interests or behaviour.

4. Use of Personal Information (s. 62 Act)

The College uses personal information about its students, staff and other third parties to carry out its mission and functions. It will not use personal information for purposes other than those identified at the time of collection, except with the consent of the person concerned.

5. Consent

In situations where consent is required, the College must transmit a consent for the collection, use or disclosure of personal information to the persons concerned. In order to be valid, consent must be clear, free and informed and be given for specific purposes, in clear and simple language, and for the duration necessary to achieve the purposes for which it was requested.

Once a person has provided consent to the collection, use and disclosure of their personal information, they may withdraw it at any time. To withdraw consent, where applicable, the person may contact the person named in the consent form (e.g. by e-mail, fax, telephone, etc.).

It should be noted that if a person withdraws its consent, the College may not be able to provide a particular service. For example, a candidate who refuses to provide consent for the transmission of their high school grades to the College may not be admitted. The College will explain to this person the impacts of withdrawing consent in order to assist them in their decision-making process.

A sample consent form can be found on the College portal, in the Legal Affairs community.

6. Release of Personal Information

a. Release without consent from the person concerned

The College may release certain personal information it holds to comply with a court order, law or legal process, including to respond to any governmental or regulatory request, in accordance with applicable law, or if the College believes that disclosure is necessary or appropriate to protect the rights, property or safety of the College or other persons.

The College may release certain personal information in its possession to a member of the College staff who is qualified to receive it where such information is necessary for the discharge of their duties.

The College may release the personal information it collects to service providers and other third parties who support the College; these third parties must be contractually obliged to keep the personal information confidential, to use it only for the purposes for which the College disclosed it, and to handle the personal information in accordance with the standards set out in this Guideline and in compliance with the applicable laws (including the Act). Such service providers or third parties must notify the person in charge of the protection of personal information at the College without delay of any violation or attempted violation of an obligation concerning the confidentiality of the information released, and must also allow the person in charge to verify compliance with confidentiality requirements. (s. 67.2 Act)

The College may release certain personal information for study or research purposes or for the production of statistics, subject to the conditions set out in the Act, including, among others, a privacy impact assessment and the transmission of the agreement to the *Commission d'accès à l'information* thirty (30) days before its coming into force (ss. 67.2.1 to 67.2.3 Act).

In certain situations, a record of the release must be made in the register of release of personal information maintained by the person responsible for the protection of personal information at the College. For greater certainty, this register must contain the following information:

i. the nature or type of information released;
ii. the person or body to which the information is released;
iii. the purpose for which the information is released and, if

applicable, a statement to the effect that it is a release of personal information referred to in section 70.1 of the Act;

iv. the reason justifying the release.

b. Release <u>with</u> consent from the person concerned

The College may release certain personal information held to a person if it has obtained the concerned person's valid consent. (See section above on consent).

7. <u>Keeping and Destruction of Personal Information</u>

The College is required to keep the personal information in its possession only for as long as necessary to fulfill the purposes for which it was collected and in accordance with its retention schedule, unless authorized or required by applicable laws or regulations. The College's retention schedule is available on the its portal, in the Legal Affairs community.

As a general rule, once the purposes for which personal information was collected or used have been achieved, the College must destroy or anonymize it to use it for public interest purposes. (s. 73(1) Act)

Information concerning a natural person is <u>anonymized</u> if it is, at all times, reasonably foreseeable in the circumstances that it no longer allows the person to be identified directly or indirectly. It should be noted that the anonymization process must be irreversible. (s. 73(2) Act)

However, as an exception to the general rule, in the case of personal information contained in a record covered by the College's retention schedule, the College must comply with the rules set out therein for the retention and disposal of such records. (s. 73(1) Act)

When the College destroys documents containing personal information, it must take the necessary protection measures to ensure the confidentiality of the information. The method of destruction used must be appropriate to the sensitivity of the information, the purpose for which it is to be used, as well as its quantity, distribution and medium. For more information, please refer to Policy No. 9 on Records Management and Archives available on the College website.

Personal information retained by the College is processed and stored <u>in Quebec</u>. Whenever possible, the College should give preference to suppliers who are able to process and store personal information within Quebec. In the event that a transfer of personal information outside Quebec is necessary in the execution of the College's functions, such transfer will only take place once it has been assessed that the

information would benefit from adequate protection, in particular in consideration of the sensitivity of the information, the purpose for which it is to be used, the protection measures that the information would benefit from, and the legal framework applicable in the state or province in which the information would be released. The transfer will also be subject to appropriate contractual arrangements to ensure such adequate protection. (s. 70.1 Act)

8. Protection of Personal Information

The College has implemented appropriate and reasonable physical, organizational, contractual and technological safeguards to protect personal information in its possession from loss or theft, and from unauthorized access, disclosure, copying, use or modification that are not authorized by the Act. The College has taken measures to ensure that only those staff members who absolutely require access to the information in the course of their duties are authorized access to it.

Persons working for or on behalf of the College have a duty, among other things, to:

i. make reasonable efforts to minimize the risk of unintentional disclosure of personal information;
ii. take special precautions to ensure that personal information is not monitored, overheard, accessed or lost when working in premises other than the College's offices;
iii. take reasonable measures to protect personal information when moving from one location to another.

Subcontractors/contractor with access to personal information that is in the possession or control of the College must be made aware of this Guideline on the Rules of Governance for the Protection of Personal Information and of other applicable policies and processes to ensure the security and protection of personal information. All subcontractors/contractors will be required to agree, in writing, to comply with all applicable directives, guidelines, policies, processes and laws.

9. Requests for Access to or Correction of Personal Information

a. Requesting access to personal information (ss. 94 and ff. Act)

Upon request, any person has the right to access personal information concerning them held by the College, subject to the exceptions set out in the Act.

A request for release can only be considered if it is made in writing by a natural person who proves that they are the person concerned or the

representative, heir or successor of that person, the liquidator of the succession, a beneficiary of life insurance or of a death benefit, the person having parental authority even if the minor child is deceased, or the spouse or close relative of a deceased person in accordance with section 88.0.1 of the Act.

This request must be addressed to the person responsible for access to documents and the protection of personal information at the College who can be reached at accesstoinformation@johnabbott.qc.ca. The request must contain sufficient specific indications to allow the College to process the request.

The person responsible for access to documents and the protection of personal information:

i. provides the person who made the written request with notice of the date the request was received;
ii. responds no later than twenty (20) days after the date of receipt of a request;
iii. if the processing of the request within the above time frame does not appear to the responsible person to be possible without interfering with the normal course of operations of the College, may extend the time frame for a period not exceeding ten (10) days by giving notice to that effect to the person who made the request, prior to the end of the initial twenty (20) day period.

If the person making the request is not satisfied with the College's response, they may refer the decision to the *Commission d'accès à l'information* for review. This request for review must be made within thirty (30) days of the date of the decision or the end of the period provided in the Act for responding to the request.

b. Request for correction (ss. 94 and ff. Act)

A person who receives confirmation of the existence of personal information concerning them on a file may request that the file be corrected if the information is inaccurate, incomplete or equivocal, or if its collection, release or keeping of the information is not authorized by the Act. (s. 89 Act)

A request for correction is made following the same procedure as that set out in paragraph 9.a above dealing with a request for access.

When the College accepts a request for correction of a file, it must issue to the person who made the request, free of charge, a copy of any amended or added personal information or, as the case may be, an attestation of the deletion of personal information. (s. 92 Act)

When the College denies the request for correction of a file, in whole or in part, the person concerned may demand that the request be recorded (s. 91 Act)

10. Management of Confidentiality Incidents

a. Definition (s. 63.8 Act)

For the purposes of this Guideline, a "confidentiality incident" is:

i. access to personal information not authorized by the Act;
ii. use of personal information not authorized by the Act;
iii. release of personal information not authorized by the Act;
iv. loss of personal information or any other breach of the protection of such information.

For purposes of clarity, **Annex A** contains a non-exhaustive list of examples of confidentiality incidents.

b. Handling of a confidentiality incident (ss. 63.7, 63.9 and 63.10 Act)

When the College has cause to believe that a confidentiality incident involving personal information it holds has occurred, the College must take reasonable measures to reduce the risk of injury and to prevent new incidents of the same nature, which may include sanctioning the individuals involved.

The College may also notify any person and/or body that could reduce this risk by releasing to such person or body only the personal information necessary for such purpose without the consent of the person concerned. In such a case, the person in charge of the protection of personal information must record the release of the information.

If the confidentiality incident presents a risk of serious injury, the body must promptly notify the *Commission d'accès à l'information*. It must also notify any person whose personal information is concerned by the incident.

In order to assess the risk of injury to a person whose personal information is concerned by a confidentiality incident, the College must consider, in particular:

i. the sensitivity of the information concerned;
ii. the anticipated consequences of its use;
iii. the likelihood that such the information will be used for injurious purposes.

The College must also consult with the person responsible for the protection of personal information.

c. Register of confidentiality incidents (s. 63.11 Act)

In accordance with the Act, the College keeps a register of confidentiality incidents. This register contains, in particular:

i. a description of the personal information covered by the incident;
ii. the circumstances of the incident;
iii. the date when the incident occurred;
iv. the date the person responsible for the protection of personal information became aware of the incident;
v. the number of persons concerned;
vi. an assessment of the risk of serious injury;
vii. if there is a risk of serious injury to the persons concerned, the dates the notices were sent;
viii. the measures taken in response to the incident.

11. Process for Dealing with Complaints Regarding the Protection of Personal Information (s. 63.3 Act)

a. Filing a complaint regarding the protection of personal information

Any person who has reason to believe that a confidentiality incident has occurred and that the College has failed to protect the confidentiality of the personal information in its possession, may file a complaint to request that the situation be rectified.

The complaint must be in writing and include a detailed description of the incident, the date or period of time when the incident occurred, the nature of the personal information affected by the incident and the number of persons involved.

The complaint shall be addressed to the person responsible for the protection of personal information.

If the complaint involves the conduct of the person responsible for the protection of personal information, the complaint shall be addressed to the Director General of the College.

b. Handling the complaint

The person responsible for the protection of personal information or the Director General, as the case may be, is responsible for processing the complaint within thirty (30) days of receipt; if the processing of the complaint is not possible within the said delay, the complainant shall be informed of the new applicable delay as soon as possible. In the event that the complaint is found to be justified, the College will take the necessary measures to correct the situation as soon as possible in accordance with paragraph 10.0 hereof (Handling of a confidentiality incident) and shall proceed with the registration of the incident in the registry, as indicated in paragraph 10.10.c hereof (Register of confidentiality incidents).

The person responsible for the protection of personal information or the Director General, as the case may be, must inform the complainant of the conclusion of the handling of the complaint.

12. Video Surveillance

The use of video surveillance must be carried out in compliance with the obligations set out, among others, in the Quebec Civil Code, the Charter of Human Rights and Freedoms, the Act and applicable College procedures.

13. Information Systems or Electronic Service Delivery System Projects Involving Personal Information (ss. 63.5 and 63.6 Act)

The College must conduct a privacy impact assessment 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. Any such assessment shall be proportionate to the sensitivity of the information concerned, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored.

In conducting a privacy impact assessment, the College must consult its Committee from the outset of the project.

14. Roles and Responsibilities

The protection of personal information held by the College is the responsibility of all College employees and it is the duty of each employee to ensure compliance with the rules contained in this Guideline. Each department of the College may adopt procedures or guidelines to clarify the application of this Guideline within their department, provided that the rules of this Guideline are respected. In the event of a discrepancy between the provisions of this Guideline and any such procedure or guideline, the provisions of this Guideline prevail. Similarly, any College by-law, policy, procedure, guideline or other document must comply with the rules of this Guideline, which shall take precedence in the event of any discrepancy.

15. Training and Awareness Activities

During the orientation session for new College employees, they will be informed of their obligations under this Guideline and the Act. Each department will also ensure that its staff is aware of this Guideline and its application as it pertains to their work. Additionally, on a regular basis and as required, the College will hold training and awareness activities on the protection of personal information in collaboration with its Professional Development (PD) office.

16. Sanctions for Non-Compliance

Failure to comply with this Guideline may result in administrative and/or disciplinary measures up to and including termination of employment. The nature, seriousness and repetitive nature of the acts complained of must be considered when determining a sanction.

In the context of its contractual relationships with a third party, the College may terminate any contract, without notice, for failure to comply with this Guideline. This Guideline will be presented to all third parties contracting with the College, who must undertake and agree in writing to comply with it.

17. Dissemination and Update

The person responsible for the protection of personal information, assisted by the Committee and the Directors' Table, will ensure that this Guideline is disseminated and updated on the College's website.

18. Responsibility

The person responsible for the protection of personal information, assisted by the Committee and the Directors' Table, will be responsible for the application of this Guideline and its review.

Without limitation, managers are responsible for the dissemination and application of this Guideline within their respective teams; and each employee has an obligation to protect the personal information held by the College and to respect the obligations contained in this Guideline.

19. Effective Date

This Guideline has been adopted by the College's Directors' Table and the Committee and will enter into effect on September 22, 2023.

ANNEX A

Examples of Confidentiality Incidents

- A staff member who accesses personal information that is not required for the performance of their duties by exceeding the access rights granted to them or a hacker breaking into a system.
- A staff member who uses personal information from a database to which they have access in the course of their duties in order to impersonate an individual.
- A person who loses documents containing personal information or has them stolen.
- A person who interferes with a database containing personal information in order to alter it.
- Forgetting to redact personal information in a document.
- Sending an e-mail containing personal information to the wrong person.
- Disclosing personal information contrary to the provisions of the Act.
- A staff member who accesses personal information without authorization.
- A staff member who communicates personal information to the wrong recipient.
- The organization is the victim of a cyber attack, such as phishing or ransomware.