CHAMPLAIN
REGIONAL COLLEGE

DIRECTIVE SERVING AS THE POLICY CONCERNING THE GOVERNANCE RULES FOR THE PROTECTION OF PERSONAL INFORMATION

This directive was adopted for the first time by the Senior Management Committee (SMC) on November 30, 2023 and subsequently amended:

Senior Management Committee (SMC)

1. PREAMBLE

The purpose of this policy is to meet the requirements *of the Regulation respecting the privacy policies of public bodies collecting personal information by technological means of the Act respecting Access* to documents held by public bodies and the Protection of personal information (CQLR, c. A-2.1) ("the Access to Information Act"), which requires the College to adopt and enforce the application of the Act by establishing the rules governing the protection of personal information that the College collects. Throughout this policy the words College, Champlain College and Champlain Regional College are understood to implicitly include the constituent colleges, i.e., Champlain College Lennoxville, Champlain College Saint-Lambert, and Champlain St. Lawrence College.

2. DEFINITIONS

PERSONAL INFORMATION

Any information that directly or indirectly identifies a natural person, such as: name, address, telephone number, email address, occupation, social insurance number, date of birth, photograph, and bank account details. Personal information must be protected regardless of the nature of the medium and regardless of its form: written, graphic, audio, visual, computerized, or otherwise.

SENSITIVE PERSONAL INFORMATION

Personal information is sensitive when, by its nature or by reason of the context in which it is used or disclosed, it gives rise to a high degree of reasonable expectation of privacy. Sensitive information includes, but is not limited to, medical, biometric, genetic, or financial information, information about sexual life or orientation, religious beliefs, or ethnic origin.

CONSENT

Consent is the authorization of the individual who owns the personal information to collect and use their personal information. Consent cannot be presumed. It must be manifest, free, informed, given for specific purposes, in simple and clear terms, for the time necessary to achieve the purposes for which it has been requested.

MINOR

Person under the age of 18.

MAJOR

Person 18 years of age and older or person under 18 years of age who is emancipated.

3. SCOPE AND LEGAL FRAMEWORK

As a public body, Champlain Regional College collects personal information, including that of students and staff. It is therefore subject to the provisions of the *Act respecting Access to documents held by public bodies and the Protection of personal information (*CQLR, c. A-2.1), the *Civil Code of Québec* (CCQ, 1991) and *the Charter of Human Rights and Freedoms* (CQLR, c. C-12). In the event of any discrepancy between the Access to Information Act and this policy, the Act prevails. This policy applies to any individual who, in the performance of their duties, collects, accesses, uses, discloses, holds, or retains personal information held by the College about any natural person.

4. COLLECTION OF PERSONAL INFORMATION

4.1 PERSONAL INFORMATION THAT MAY BE COLLECTED

To properly fulfill its mission, Champlain Regional College must collect a number of pieces of personal information.

The College collects only the personal information necessary for the performance of its duties or functions or for the implementation of a program under its control.

The College may also collect personal information if it is necessary for the exercise of its powers, duties, or the implementation of a program of the public body with which it collaborates for the provision of services or for the achievement of a common mission. In such a case, the collection must be preceded by a privacy impact assessment and be carried out within the framework of a legal agreement sent to the *Commission d'accès à l'information du Québec* in accordance with the Access to Information Act.

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

4.2 INFORMATION DISCLOSED WHEN COLLECTING PERSONAL INFORATMATION

When it collects personal information, the College ensures that the individual concerned is informed, at the latest at the time of collection:

4.2.1 The name of the public body on whose behalf the collection is being made;
4.2.2 The purposes for which the information is collected;
4.2.3 The means by which the information is collected;
4.2.4 Whether the request for information is mandatory or optional;
4.2.5 Consequences of refusing to respond to or consent to the request;
4.2.6 The rights of access and rectification provided for in the Act;
4.2.7 The possibility that personal information may be communicated outside of Québec, if applicable.

Upon request, the person concerned is also informed of the personal information collected from them, the categories of persons who have access to it within the public body, the period for which this information is kept and the contact information of the person responsible for the protection of personal information.

5. USE OF PERSONAL INFORMATION

The College uses personal information about its students, employees and other third parties to carry out its mission and functions. Personal information will not be used for purposes other than those identified at the time of collection, except with the express consent of the individual who owns the personal information or as required by the Access to Information Act.

6. CONSENT

In situations that require it, the College is required to request consent to the collection, use or disclosure of personal information from the individuals concerned. To be valid, consent must be manifest, free, informed, given for specific purposes, in simple and clear terms and for the time necessary to achieve the purposes for which it is requested.

Once an individual has provided consent to the collection, use and disclosure of their personal information, they may withdraw their consent at any time. To withdraw consent, if applicable, they may contact the person named on the consent form. If so, the College will explain to the individual the impact of withdrawing consent to assist them in their decision-making.

7. DISCLOSURE OF PERSONAL INFORMATION

7.1 DISCLOSURE WITHOUT CONSENT

The College may disclose certain personal information held in order to comply with a court order, a law, or a legal process, including to respond to any governmental or regulatory request, in accordance with applicable laws, or if the College believes disclosure is necessary or appropriate to protect the rights, property or safety of the College or others.

The College may disclose certain personal information in its possession to a member of the College's staff who is qualified to receive it and when the information is necessary for the performance of their duties.

The College may transfer the personal information it collects to service providers and other third parties that support the College. These third parties are contractually obligated to keep personal information confidential, to use it only for the purposes for which the College discloses it, and to treat personal information in accordance with the standards set out in this policy and in accordance with the law.

The College may disclose certain personal information for the purposes of study, research, or the production of statistics subject to the conditions set out in the Access to Information Act, including, in particular, the 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 in accordance with the provisions of the Access to Information Act (articles 67.2.2 to 67.2.3).

In certain situations, the person responsible for the protection of personal information must record the disclosure in the College's privacy record.

7.2 DISCLOSURE WITH CONSENT

The College may disclose certain personal information it holds to a person if it has obtained the meaningful consent of the individual.

8. CONSERVATION AND DESTRUCTION OF PERSONAL INFORMATION

The College retains the personal information it holds 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.

Generally, when the purposes for which personal information was collected or used are fulfilled, the College must destroy or anonymize it for use in the public interest.

Information about an individual is anonymized when it is, at any time, reasonable to foresee in the circumstances that it can no longer be directly or indirectly identified by that individual. It should be noted that the anonymization process must be irreversible.

However, as an exception to the general rule, if the personal information is contained in a document that is subject to the College's retention schedule, the College must comply with the rules set out in the document regarding the retention and destruction of such records.

When the College destroys documents containing personal information, it ensures that it takes the necessary safeguards to ensure the confidentiality of the information. The method of destruction used must be determined based on the sensitivity of the information, the purpose for which it was used, the amount, the distribution and the medium of the information.

Personal information held by the College is processed and stored in Quebec. In the event that a transfer of personal information outside Québec is necessary in the course of carrying out the functions of the College, such transfer will only take place if it is assessed that the information would benefit from adequate protection, in particular by considering the sensitivity of the information, the purpose of its use, the protection measures from which the information would benefit and the legal regime applicable in the state or province where the information is provided would be communicated. The transfer will also be subject to appropriate contractual arrangements to ensure this adequate protection.

9. PROTECTION OF PERSONAL INFORMATION

The College has put in place appropriate and reasonable physical, organizational, contractual, and technological security measures to protect the personal information in its custody against loss or theft, and against unauthorized access, disclosure, copying, use, or modification. The College has taken steps to ensure that only those members of its staff who absolutely need to have access to personal information in the custody of the College in the course of their duties are authorized to access it.

Persons who work for or on behalf of the Cégep must, among other things:

- Provide reasonable efforts to minimize the risk of unintentional disclosure of personal information;
- Take special precautions to ensure that personal information is not monitored, heard, accessed, or lost while working in premises other than the College's offices; and
- Take reasonable steps to protect personal information when moving from one location to another.

Subcontractors with access to personal information in the custody or control of the College will be informed of this Privacy Policy and other applicable policies and processes to ensure the security and protection of personal information. All subcontractors must agree in writing to comply with applicable policies, processes and laws.

10. REQUESTS FOR ACCESS TO OR CORRECTION OF PERSONAL INFORMATION

10.1 REQUESTS FOR ACCESS TO PERSONAL INFORMATION

Upon request, an individual has the right of access to his or her personal information held by the College, subject to the exceptions set out in the Access to Information Act.

A request for access can only be considered if it is made in writing by a natural person who can prove that they are the subject of the request, or are acting as a representative, an heir or successor to the person, as a liquidator of the estate, as a beneficiary of a life insurance policy or a death benefit, as the holder of parental authority even if the minor child is deceased, or as the spouse or close relative of a deceased person.

This request should be addressed to the Secretary General who is responsible for the protection of personal information held by the College, who can be reached at the **Champlain Administrative Services, 1301 Portland Blvd., Sherbrooke, Quebec, J1J 1S2 corporateaffairs@crcmail.net .** The application must provide sufficient specific information to enable the College to process it.

The Secretary General must give the person who made a written request an acknowledgement including the date of receipt of the request.

The Secretary General must respond no later than twenty (20) days from the date of receipt of a request. If it is not possible to process the request within the time limit set out above without interfering with the normal course of the College's activities, the Secretary General may extend the request for a period not exceeding ten (10) days by giving notice to that effect to the applicant before the expiry of the 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 expiry of the time limit set out in the Access to Information Act to respond to the request.

10.2 REQUEST FOR CORRECTION TO PERSONAL INFORMATION

An individual who receives confirmation of the existence of personal information about them in a file

held by the College and if this personal information is inaccurate, incomplete, or ambiguous, or if the collection, disclosure, or retention of this personal information is not authorized by the Access to Information Act, may request that the file be corrected.

A request for rectification can only be considered if it is made in writing by a natural person who can prove that they are the data subject of the request, or are acting as a representative, an heir or successor to the person, or a liquidator of the estate, as a beneficiary of life insurance or death benefit, as the holder of parental authority even if the minor child is deceased, or as the spouse or close relative of a deceased person.

This request should be addressed to the Secretary General, who is responsible for the protection of personal information held by the College, who can be reached at the **Champlain Administrative Services, 1301 Portland Blvd., Sherbrooke, Quebec, J1J 1S2 corporateaffairs@crcmail.net.** The application must provide sufficient specific information to enable the College to process it.

The College must, when it accedes to a request for rectification of a file, issue to the person who made the request a copy of any amended or added personal information, or a certificate of the removal of personal information, free of charge.

When the College refuses, in whole or in part, to comply with a request for rectification of a file, the person concerned may request that this request be registered.

The Secretary General must respond no later than twenty (20) days from the date of receipt of a request. If it is not possible to process the request within the time limit set out above without interfering with the normal course of the College's activities, the Secretary General may extend the request for a period not exceeding ten (10) days by giving notice to that effect to the applicant before the expiry of the 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 expiry of the time limit set out in the Access to Information Act to respond to the request.

11. BREACH OF PRIVACY INCIDENT MANAGEMENT

11.1 DEFINITION

According to this policy, a breach of privacy incident is:

1. Access to personal information not authorized by the Access to Information Act;
2. Use of personal information not authorized by the Access to Information Act;
3. Disclosure of personal information not authorized by the Access to Information Act;
4. Disclosure of personal information made in error to the wrong recipient;
5. Loss of personal information or other breach of personal information.

11.2 HANDLING A BREACH OF PRIVACY INCIDENT

When the College has reason to believe that a breach of privacy incident involving personal

information under its control has occurred, it must take reasonable steps to reduce the risk of harm being caused and to prevent future incidents of the same nature from occurring, which may include sanctioning the individuals involved.

The College may also notify any person and/or organization likely to reduce this risk by disclosing only the personal information necessary for this purpose without the consent of the person concerned. In this case, the Secretary General must record the breach.

If the breach of privacy incident presents a risk of serious harm, the College must, with due diligence, notify the *Commission de l'accès à l'information*. It must also notify any person whose personal information is affected by the incident.

To assess the risk of harm to an individual whose personal information is affected by a breach of privacy incident, the College must consider, among other things:
1. The sensitivity of the information concerned;
2. The anticipated consequences of its use; and
3. The likelihood that it will be used for a harmful purpose.

The College must also consult with the Secretary General.

11.3 BREACH OF PRIVACY INCIDENT LOG

The College maintains a log of breach of privacy incidents. It contains, in particular:
1. A description of the personal information involved in the incident;
2. The circumstances of the incident;
3. The date on which the incident took place;
4. The date on which the Secretary General became aware of the incident;
5. The number of people targeted;
6. The assessment of the severity of the risk of harm;
7. If there is a risk of serious harm to the data subject, the dates on which the notices were sent; and,
8. The actions taken in response to the incident.

12. BREACH OF PRIVACY COMPLAINT PROCESS

12.1 FILING A BREACH OF PRIVACY COMPLAINT

Anyone who has reason to believe that a breach of privacy incident has occurred and that the College has failed to protect the confidentiality of the personal information it holds may file a complaint requesting that the situation be corrected.

The complaint must be made in writing and include a description of the incident, the date or period in which the incident occurred, the nature of the personal information involved in the incident, and the number of individuals involved.

This complaint should be addressed to the Secretary General, who is responsible for the protection of personal information held by the College, who can be reached at the **Champlain Administrative Services, 1301 Portland Blvd., Sherbrooke, Quebec, J1J 1S2** **corporateaffairs@crcmail.net** **.** The complaint must provide sufficient specific information to enable the College to process it.

If the complaint involves the conduct of the Secretary General (the person responsible for the protection of personal information), it must be addressed to the College's Director General.

12.2 HANDLING OF THE COMPLAINT

It is the responsibility of the Secretary General or the Director General, as applicable, to deal with the complaint within fifteen (15) days of the date of receipt of the complaint. If the complaint is considered to be well-founded, the College will take the necessary measures to correct the situation as soon as possible in accordance with paragraph 11.2 of this policy and will record the incident in the log as indicated in paragraph 11.3.

13. VIDEO SURVEILLANCE

The use of video surveillance must be carried out in accordance with the College's *Video Surveillance Policy*, in compliance with the obligations set out in the *Civil Code of Québec,* the *Charter of Human Rights and Freedoms* and the Access to Information Act.

14. INFORMATION SYSTEM OR ELECTRONIC SERVICE DELIVERY PROJECTS INVOLVING PERSONAL INFORMATION

The College conducts a privacy impact assessment for any project to acquire, develop or redesign an information system or electronic service delivery that would involve the collection, use, disclosure, retention, or destruction of personal information.

With respect to the Privacy Impact Assessment, the College consults with its Access to Information and Privacy Committee at the outset of the project.

15. ROLES ET RESPONSIBILITIES

15.1 BOARD OF GOVERNORS AND EXECUTIVE COMMITTEE

The Board of Governors adopts this policy and its amendments. The Board is regularly informed of the College's initiatives and developments regarding the protection of personal information. The Board is responsible for the application of this policy.

15.2 SENIOR MANAGEMENT COMMITTEE (SMC)

The Senior Management Committee (SMC) determines measures to promote the implementation of this policy. Thus, it determines the strategic orientations, the action plan and the risk assessments of college governance rules relating to the protection of personal information. The committee may also determine guidelines and procedures that clarify or support the application of this policy.

15.3 INFORMATION RESOURCES GOVERNANCE COMMITTEE

The purpose of the Information Resources Governance Committee is to assist the Information Security Officer (RSI) and the Secretary General with the implementation of the governance rules relating to the protection of persona! information and to comply with the regulations.

This committee is responsible for developing the awareness-raising or training activities and any proposals for action on protecting persona! information.

15.4 DIRECTOR GENERAL

The Director General oversees the application of this policy and is responsible for:

a) Delegates certain responsibilities to the Secretary General for the management of information;
b) Making recommendations to the Board of Governors regarding the adoption of strategic orientations, risk assessment, action plans, information security health assessments, accountability on information security and breaches;
c) Authorizing an investigation where there is, or could be, an actual or apparent violation of this policy;
d) Investigating when a complaint is made implicating the Secretary General as stated in article 12.1 of this policy.
e) Ensuring the maintenance of the log of breach of privacy incidents.

15.5 POSITION RESPONSIBLE FOR THE PROTECTION OF PERSONAL INFORMATION

The position responsible for the protection of personal information is the Secretary General. The Secretary General, with the approval of the Director General, may delegate all or part of their responsibility to another member of their department or service.

15.6 POSITION RESPONSIBLE FOR DOCUMENT MANAGEMENT AND ARCHIVES

The person responsible for document management may delegate all or part of their responsibility to another member of their department or service;

The person responsible for document management and archives:

- Informs the employees under their authority as well as third parties with whom the service interacts, of the governance rules relating to the protection of personal information;
- Oversees the protection of personal information under their responsibility and ensuring that these are used by employees under their authority in accordance with this policy and any other element of the management framework;
- Conducts a privacy impact assessment for any project to acquire, develop or redesign an information system or electronic service delivery that would involve the collection, use, disclosure, retention, or destruction of personal information.
- Reports immediately any confidentiality incident to the person responsible for the protection of personal information;
- Reports to the Director General any problem associated with the application of this policy including any actual or apparent violation by an employee in the application of this policy.

15.7 USERS

Any user who accesses, consults, deals with, or manages personal information is responsible for its use and must proceed in such a way as to protect it.

To this end, users must:

- Comply with this policy and any other directive of the College on the protection of personal information and its use;
- Use the access rights granted and authorized, the information and the information systems that are available solely in the course of their duties and for the purpose for which they are intended;
- Participate in the categorization of personal information within their department or service;
- Respect the measures in place to protect personal information such as but not limited to, not circumventing them, changing their configuration, or disabling them;
- Inform the Secretary General of any incident likely to constitute a violation of this policy or to constitute a threat to the protection of persona! information;
- Collaborate in any intervention to identify or mitigate a threat to the protection of persona! information or a breach of privacy incident.

As a result, all College users must comply with the policies and directives in their professional or academic activities when sharing information assets, information technology or information systems.

16. PRIVACY TRAINING AND AWARENESS ACTIVITIES OFFERED BY THE COLLEGE TO ITS STAFF

Each year, the college will conduct at least one training and awareness activity for its management personnel.

17. PENALTIES FOR NON-COMPLIANCE WITH THIS POLICY

Failure to comply with this policy may result in administrative and/or disciplinary action. The nature, seriousness and repetitive nature of the alleged acts will be considered when determining a sanction.

As part of its contractual relationship with a third party, the College may terminate any contract without notice for non-compliance with this policy. This will be presented to all third-party contractors with the College, who will have to undertake, in writing, to comply with it.

18. DISSEMINATION AND UPDATING OF THE POLICY

The Secretary General, assisted by the Access to Information and Privacy Committee, ensures that the policy is posted and updated on the Management Committee's website.

19. RESPONSIBILITY FOR THE APPLICATION AND REVISION OF THE POLICY

The Secretary General, as Privacy Officer, is responsible for the application and revision of this policy.

20. COMING INTO FORCE

This policy is recommended by the Access to Information and Privacy Committee to Senior Management Committee and comes into effect on the day it is adopted by the Board of Governors or by November 30, 2023, whichever comes first.