Administrative Policies – Table of Contents

College of Paramedics of Nova Scotia

Policy Name:	Confidentiality of College of Paramedics of Nova Scotia Information		
Policy Number:	Administrative – 1.0		
Version Number:	1	**Date first Approved:**	09/28/2021
Approved by:	ED/Registrar	**Effective Date:**	09/28/2021
Version Date:	09/28/2021	**Next Review Date:**	09/28/2021

DEFINITIONS

"College" means the College of Paramedics of Nova Scotia.

"Confidential Information" means all confidential, non-public or proprietary information, data, documents, and other materials in whatever form (including, without limitation, in written, oral, visual or electronic form), whether or not such information is marked confidential, that relates to the College, its members, employees, Council members, committee and/or working group members, applicants, complainants, respondents, stakeholders, and/or third parties, including (without limitation):

- Personal Information, including personnel records and payroll records.
- Computer system passwords and security codes.
- Research results not yet published including manuscripts and correspondence.
- Budgetary, service area or College planning information.
- Litigation pending or in process.
- Other sensitive information including intellectual research findings, intellectual property and financial data.

"Council" means the Council of the College.

"Employee" means any individual employed by the College, whether on a permanent, temporary or part-time basis.

"Personal Information" has the meaning ascribed to it in the College's "Privacy Policy".

"Privacy Breach" has the meaning ascribed to it in the College's "Responding to a Breach of Privacy Policy".

"Third-Party Service Provider" means any individual or entity that provides services to the College and is not employed by the College.

"Volunteer" means any individual who volunteers with the College, including without limitation any member of the Council, or any member of any committees or working groups of the College.

POLICY STATEMENT

1. This policy applies to:
   1.1. All Employees;
   1.2. All Volunteers;
   1.3. All Third-Party Service Providers of the College;
   1.4. All Confidential Information of the College, or in its custody or control.

2. The College will adhere to its obligations related to its handling and protection of Confidential Information in its possession and control, and to ensure Employees, Council members, Volunteers, and Third-Party Service Providers of the College are knowledgeable and fully informed of their obligations with respect to Confidential Information.

3. The College protects and safeguards Confidential Information entrusted to it by Employees, Volunteers, members, applicants, stakeholders and other third parties from unauthorized access, use, and disclosure.

4. All Employees and Volunteers shall sign a confidentiality agreement with the College.
5. During the term of employment or term of office, and after termination, all Employees and Volunteers have a duty to keep confidential and protect against unauthorized use or disclosure all Confidential Information, in accordance with the confidentiality agreement.

6. All Third-Party Service Providers with access to Confidential Information shall sign an independent contractor agreement prior to being given access to such information.
   6.1. During the Third-Party Service Provider's engagement with the College, and after termination, all Third-Party Service Providers have a duty to keep confidential and protect against unauthorized use or disclosure all Confidential Information, in accordance with the independent contractor agreement.

7. Confidential Information shall be kept in safe and secure places and shall not be accessible to public view.

8. Computerized records with limited user access and computer terminals shall not be accessible to other than authorized users.

9. Any Personal Information shall only be collected, used, accessed, stored, and disclosed in accordance with the College's "Privacy Policy", and any Privacy Breach shall be handled in accordance with the College's "Responding to a Breach of Privacy Policy".

10. If an individual or entity has not given their signed consent for the College to disclose their Confidential Information to another source, such consent will be sought, or the information will not be divulged unless the College is legally required to do so.

11. Unauthorized use and disclosure of Confidential Information may lead to disciplinary action including immediate termination.

12. In order to ensure protection of the College's Confidential Information, and Confidential Information in its custody or control, the Privacy Officer is responsible for managing all inquiries from any third party, including (without limitation) the press and/or media, regarding the College or Confidential Information.
    12.1. All such inquires will be immediately referred to the Privacy Officer.

RELATED DOCUMENTS
Policy Adm 1.0 – Confidentiality of College of Paramedics of Nova Scotia Information
Attachment A – Confidentiality Agreement

DOCUMENT HISTORY ((Date of Reviews. Revisions, etc):

Attachment A

Confidentiality Agreement

This Confidentiality Agreement is entered into, by the signatory, on the below date. This agreement applies to all:

- Employees.
- Volunteers.
- Third-party Service Providers of the College.
- Confidential information of the College, or in its custody and control.

In this agreement "Confidential Information" means all confidential, non-public or proprietary information, data, documents, and other materials in whatever form (including, without limitation, in written, oral, visual or electronic form), whether or not such information is marked confidential, that relates to the College, its members, employees, Council members, committee and/or working group members, applicants, complainants, respondents, stakeholders, and/or third parties, including (without limitation):

- Personal Information, including personnel records and payroll records.
- Computer system passwords and security codes.
- Research results not yet published including manuscripts and correspondence.
- Budgetary, service area or College planning information.
- Litigation pending or in process.
- Other sensitive information including intellectual research findings, intellectual property, and financial data.

"Personal Information" means any information about an identifiable individual or information that, when combined with other information, whether readily available or not, may identify or tend to identify an individual, as may be defined or limited under applicable privacy legislation. Personal Information does not include anonymous or de-identified data that is not associated with a particular individual.

I have read and been provided with the opportunity to obtain additional information regarding the following Administrative Policies of the College:

- 1.0 Confidentiality of College of Paramedics of Nova Scotia Information
- 1.1 Privacy Policy
- 1.2 Collection and Use of Employee Personal Information
- 1.3 Responding to a Privacy Breach

I understand that as a signatory to this agreement I:

- Have a duty to handle and protect confidential information in my possession and control.
- Am knowledgeable and fully informed of my obligation with respect to confidential information in my possession and control.

- Must keep confidential and protect against unauthorized use or disclosure of confidential information.
- Will keep confidential information in a safe and secure place and shall ensure it is not accessible to public view.
- Shall not allow unauthorized access to computerized records with limited user access and/or computer terminals, or other electronic devices.
- Shall only collect, use, access, store and disclose personal information in accordance with the College's "Privacy Policy" and that any privacy breach shall be handled in accordance with the College's "Responding to a Breach of Privacy Policy".
- Must seek consent from an individual or entity who has not provided their signed consent for the College to disclose their Confidential Information to another source, otherwise the information will not be divulged unless the College is legally required to do so.
- Understand that unauthorized use and disclosure of Confidential Information may lead to disciplinary action including immediate termination.
- Understand the Privacy Officer is responsible for managing all inquiries from any third-party, including (without limitation) the press and/or media, regarding the College or Confidential Information and will refer all such inquiries to the Privacy Officer.

I acknowledge that any violation of this agreement could cause harm to the College and frustrate the College's work. Therefore, as a signatory to this agreement I recognize that unauthorized use and disclosure of Confidential Information my lead to disciplinary action including immediate termination.

I will direct any questions regarding my confidentiality obligations to the Executive Director/Registrar. I have read and understand the above expectations within this agreement and more broadly within the Confidentiality and Privacy Policies of the College and agree to abide by this duty of confidentiality.

Signatory:

_____

Print Name

_____ _____

Signature *Date*

College Staff:

_____

Print Name

_____ _____

Signature *Date*

Policy Name:	Privacy		
Policy Number:	Administrative – 1.1		
Version Number:	1	**Date first Approved:**	09/28/2021
Approved by:	ED/Registrar	**Effective Date:**	09/28/2021
Version Date:	09/28/2021	**Next Review Date:**	09/28/2021

DEFINITIONS

"Act" means the *Paramedics Act* (Nova Scotia).

"College" means the College of Paramedics of Nova Scotia.

"CSA Model Code" means the Canadian Standards Association Model Code for the Protection of Personal Information.

"Personal Information" means any information about an identifiable individual or information that, when combined with other information, whether readily available or not, may identify or tend to identify an individual, as may be defined or limited under applicable privacy legislation. Personal Information does not include anonymous or de-identified data that is not associated with a particular individual.

"Privacy Officer" means the Executive Director/Registrar of the College, or their designate.

POLICY STATEMENT

1. The College is committed to protecting the privacy and security of the Personal Information and is accountable for all Personal Information under its control.

2. The College will adhere to the CSA Model Code with respect to the Personal Information of its registrants and applicants to the College, as well as complainants and third parties who provide Personal Information to the College.

3. This policy does not apply to employees of the College.

Accountability

4. The College is accountable for all Personal Information under its control.

5. The College collects, uses and discloses Personal Information in accordance with its obligations under the *Act* and the CSA Model Code.

6. The College has designated a Privacy Officer, who is responsible for everyday operation and control of Personal Information and the College's compliance with this policy.

7. From time to time, the College discloses Personal Information to third parties for administrative and licensing purposes.

8. Third parties are required to sign confidentiality agreements which reinforce the strict confidentiality obligations on them.

Identifying Purposes

9. The College is required, pursuant to the *Act*, to regulate the practice of paramedicine in the province of Nova Scotia with due regard to the public interest.
   9.1. The College collects and uses Personal Information to carry out this function, or otherwise as permitted or required under applicable law.

10. The types of information (including Personal Information) the College may collect from its registrants and applicants include:
    10.1. Names, addresses, telephone numbers, email addresses, or other contact information.
    10.2. Date of birth, social insurance number, age, marital status, race, national or ethnic origin and religion.
    10.3. Educational information, such as educational program name and graduation year, proof of program completion, proof of entry to practice exam completion.
    10.4. Previous licensure status.
    10.5. Previous and current employment information.
    10.6. Language proficiency.
    10.7. Opinions about or decisions regarding the member or applicant, including academic and/or professional references, clinical and competence assessments, mental health and physical health assessments, professional conduct and/or registration/licensing decisions of the College, and decisions from another regulatory body.
    10.8. Criminal record checks and vulnerable sector checks.

11. In the event of a complaint, the College may collect Personal Information from or about the complainant, including:
    11.1. Names, addresses, telephone numbers, email addresses, or other contact information.
    11.2. Personal health information contained in patient care records.

12. The purposes for which the College collects and uses Personal Information include:
    12.1. Registration and licensing applications and renewals.
    12.2. Credentials verification and assessment, which may include sharing of Personal Information with other regulatory bodies in Canada.

12.3. Recording registrant and registrant status and establishing and maintaining updated member listings to publish on the College website and made available to inquirers.
12.4. Complaints and investigations.
12.5. Communication with registrants and applicants.
12.6. Regulatory processes.
12.7. Communication with registrants.
12.8. Publication distribution.
12.9. Compilation of statistics.
12.10. Payment of the annual licensing fee.
12.11. Surveys.

13. If the College wishes to use Personal Information for a purpose not identified, the new purposes will be identified and the College will seek consent prior to use, unless required or permitted by law.

Consent

14. The College is dedicated to ensuring that registrants, applicants, complainants and other third parties are aware of the purposes for which Personal Information is collected, the use of the information and reasons for disclosure.
    14.1. The College obtains consent from individuals for the collection, use and disclosure of Personal Information.
    14.2. In certain circumstances, the consent for the individual can be obtained after collection of the information, but before use.

15. The College will not, as a condition of the supply of goods or services, require that an individual consent to the collection, use, or disclosure of information beyond what is required for legitimate and communicated purposes.
    15.1. Some information related to licensing, competence and professional development must be provided as a condition of obtaining and maintaining one's professional status.

16. There may be circumstances where consent may be implied.
    16.1. In such cases, the purpose for the collection and use of Personal Information must be apparent and the College may only use the Personal Information for the apparent purpose.
    16.2. In such a case, the College will not use that information for any other purpose.

17. The law provides certain exceptions to the usual requirement to obtain an individual's consent. For example, an organization may collect and use Personal Information in circumstances where the collection and/or use of such information is clearly in the interests of the individual and consent cannot be obtained in a timely way.
    17.1. Similarly, Personal Information may be collected and used without the consent of the individual if the information is reasonably required to investigate a breach of an

agreement, a violation of the law or investigations related to professional discipline and there is reason to believe that obtaining consent may compromise the availability or accuracy of such information.

18. Individuals can withdraw consent at any time for the retention and use of Personal Information, but only to the extent that such consent withdrawal does not affect the ability of the College to carry out its statutory functions or comply with its obligations under law.
    18.1. The College will inform the individual of the implications of such withdrawal.

Limiting Collection

19. The College collects Personal Information only to the extent necessary for the purposes identified.
    19.1. Personal information is collected in a fair and lawful manner.

Limiting Use, Disclosure and Retention

20. The College does not sell or trade Personal Information to third parties.
    20.1. Personal Information is only used or disclosed for the purpose for which it was collected with the consent of the individual, or as required by law.
    20.2. The College discloses Personal Information to the following third parties for the following purposes:
        20.2.1. Nova Scotia Department of Health and Wellness for use in the electronic health record "Provider Registry" and paramedic human resources planning.
        20.2.2. Canadian Institute of Health Information (CIHI) for statistical health reporting.
        20.2.3. Yardstick Assessment Strategies Inc., and Canadian Organization of Paramedic Regulators for exam purposes.

21. In addition, and in accordance with its statutory obligations, the names of the College's registrants, their registration number, their active practicing status, as well as any licensing conditions, restrictions and/or sanctions applicable to the member, are made available to the public, including by posting on the College's website.

22. Except as otherwise permitted or required by applicable law or regulation, the College will only retain Personal Information for as long as necessary to fulfil the purposes for which it was collected, including for the purposes of satisfying any legal, accounting, or reporting requirements.

Accuracy

23. The College is dedicated to maintaining the Personal Information under its control in a form that is accurate, complete, and current as is necessary for the fulfilment of the College's purposes.

23.1. Individuals are encouraged to contact the College and update any changes in their Personal Information.

Safeguards

24. The College takes reasonable steps to ensure that Personal Information is protected against loss, unauthorized access, use, disclosure, and alteration.
    24.1. This protection applies to both electronic and hard copy form.
    24.2. The safeguards used by the College include:
        24.2.1. Technological measures, such as the use of passwords and data encryption for electronic information.
        24.2.2. Physical measures, such as locked filing cabinets and restricted access to areas where Personal Information is stores.
        24.2.3. Organizational measures, such as employee training, confidentiality agreements and limited access on a "need to know" basis.
        24.2.4. Third party measures, such as confidentiality agreements with third parties.
        24.2.5. Destruction measures, such as on-site shredding and physical destruction of hard drives.

Openness

25. The College is open about its policies and procedures and will provide individuals with specific information relating to the maintenance of Personal Information.
    25.1. These policies are available by contacting the College's Privacy Officer.

Individual Access

26. Individuals may contact the Privacy Officer at any time to discuss access to their Personal Information under the control of the College.
    26.1. Upon written request, access will be provided. A small fee may be applied to cover the cost of administration.
    26.2. In certain situations, such as legal or regulatory requirements, the College may not be able to offer the individual access to their Personal Information and, in such cases, the College will provide the individual with the reasons for denial.
    26.3. The College will correct or amend Personal Information that is shown to be incomplete or inaccurate.

Challenging Compliance

27. The Privacy Officer is responsible for overseeing compliance with this privacy policy.
    27.1. Any questions can be directed to the Privacy Officer who will respond to any concerns.
    27.2. The College will investigate all complaints and will take appropriate action to resolve the issue to your satisfaction.

27.3. Comments and suggestions regarding this policy are welcome.

RELATED DOCUMENTS

Policy Adm 1.0 – Confidentiality of College of Paramedics of Nova Scotia Information
Attachment A – Confidentiality Agreement

DOCUMENT HISTORY ((Date of Reviews. Revisions, etc):

Policy Name:	Collection and Use of Employee Personal Information		
Policy Number:	Administrative – 1.2		
Version Number:	1	**Date first Approved:**	09/28/2021
Approved by:	ED/Registrar	**Effective Date:**	09/28/2021
Version Date:	09/28/2021	**Next Review Date:**	MM/DD/YYYY

DEFINITIONS

"College" means the College of Paramedics of Nova Scotia.

"Council" means the Council of the College.

"Employee" has the meaning ascribed to it in the College's "Confidentiality of CPNS Information Policy".

"Personal Information" means any information about an identifiable individual or information that, when combined with other information, whether readily available or not, may identify or tend to identify an individual, as may be defined or limited under applicable privacy legislation. Personal Information does not include: (i) an Employee's business contact details and job title; or (ii) anonymous or de-identified data that is not associated with a particular individual.

"Privacy Officer" means the Executive Director/Registrar of the College, or their designate.

"Third-Party Service Provider" has the meaning ascribed to it in the College's "Confidentiality of CPNS Information Policy".

"Volunteer" has the meaning ascribed to it in the College's "Confidentiality of CPNS Information Policy".

POLICY STATEMENT

1. The College is committed to protecting the privacy and security of Employee Personal Information.
   1.1. This policy describes the categories of Personal Information that the College collects, how the College uses the Personal Information, how the College secures the Personal Information, when the College may disclose the Personal Information to third parties, and when the College may transfer the Personal Information outside of Canada.
   1.2. The College will only use the Personal Information of its Employees in accordance with this policy unless otherwise required by applicable law.

1.3. The College will take steps to ensure that the Personal Information that it collects is adequate, relevant, not excessive, and used for limited purposes.

2. This policy applies to current and former Employees of the College.

Collection of Personal Information

3. To carry out its activities and obligations as an employer, the College may collect, store, and use the following categories of Personal Information, which we require to administer the employment relationship with its Employees:
   3.1. Personal contact details such as name, title, addresses, telephone numbers, personal email addresses.
   3.2. Date of birth.
   3.3. Gender.
   3.4. Marital and dependent status.
   3.5. Beneficiary and emergency contact information.
   3.6. Government identification numbers such as social insurance or other national insurance number, driver's license number, or other identification card number.
   3.7. Bank account details and payroll information.
   3.8. Wage and benefit information.
   3.9. Compensation history.
   3.10. Performance information.
   3.11. Insurance enrolment information.
   3.12. Start date.
   3.13. Employment location.
   3.14. Education and training.
   3.15. Employment records (including professional memberships, references, work history, and proof of work eligibility).
   3.16. Photograph.
   3.17. Other personal details included in a resume or cover letter.

Use of Personal Information

4. The College will only use Personal Information where applicable law permits or requires it, for example, when necessary for the performance of the employment contract with the Employee, or when the use is necessary to comply with a legal obligation that applies to the College.
   4.1. The College may use Personal Information for the following legitimate business purposes:
      4.1.1. Employee administration (including payroll and benefits administration).
      4.1.2. Business management and planning.
      4.1.3. Processing Employee work-related claims (for example, insurance and worker's compensation claims).
      4.1.4. Accounting and auditing.

4.1.5. Conducting performance reviews and determining performance requirements.
4.1.6. Assessing qualifications for a particular job or task.
4.1.7. Gathering evidence for disciplinary action or termination.
4.1.8. Complying with applicable law.
4.1.9. Education, training, and development requirements.
4.1.10. Health administration services.
4.1.11. Complying with health and safety obligations.

5. The College will only use Personal Information for the purposes for which it was collected.
   5.1. If the College needs to use Personal Information for an unrelated purpose, the College will notify the Employee and, if required by law, seek the Employee's consent.
   5.2. The College may use Personal Information without Employees' knowledge or consent where required by applicable law or regulation.

Disclosure of Personal Information

6. The College will only disclose Personal Information to third parties where required by law or to the College's Employees, Volunteers and Third-Party Service Providers who require it to assist the College with administering the employment relationship with the Employee, including Third-Party Service Providers who provide services to the College or on the College's behalf.
   6.1. Third-Party Service Providers include, but are not limited to, payroll processors and benefits administration providers. These Third-Party Service Providers may be located outside of Canada.

7. The College requires all of its Third-Party Service Providers to implement appropriate security measures to protect Personal Information consistent with the College's policies and any data security obligations applicable to the College.
   7.1. The College permits its Third-Party Service Providers to use Personal Information only for specified purposes in accordance with the College's instructions, and not for their own purposes.

8. The College may also disclose Personal Information for the following additional purposes where permitted or required by applicable law:
   8.1. To comply with legal obligations or valid legal processes such as search warrants, subpoenas, or court orders. When Personal Information is disclosed to comply with a legal obligation or legal process, the College will take reasonable steps to ensure that only the minimum Personal Information necessary for the specific purpose and circumstances is disclosed.
   8.2. During emergency situations or where necessary to protect the safety of persons.
   8.3. Where the Personal Information is publicly available.
   8.4. For additional purposes with your consent where such consent is required by law.

Security

9. The College has implemented appropriate physical, technical, and organizational security measures designed to secure Personal Information against accidental loss and unauthorized access, use, alteration, or disclosure.
   9.1. In particular, all Employee Personal Information is maintained in electronic form, safeguarded using password protection, and secured within the College's Microsoft 365 One-drive system.
   9.2. Any paper documents completed by Employees containing Personal Information shall be scanned and maintained in accordance with the foregoing, and the paper documents shall then be destroyed by shredding.

10. In addition, the College limits Personal Information access to those Employees, Volunteers and Third-Party Service Providers, and other third parties that have a legitimate business need for such access.

Retention

11. Except as otherwise permitted or required by applicable law or regulation, the College will only retain Personal Information for as long as necessary to fulfil the purposes for which it was collected, including for the purposes of satisfying any legal, accounting, or reporting requirements.
   11.1. Under some circumstances the College may anonymize Personal Information so that it can no longer be associated with the Employee.
      11.1.1. The College reserves the right to use such anonymous and de-identified data for any legitimate business purpose without further notice to the Employee and without their consent.
   11.2. Once an individual is no longer an Employee of the College, the College will retain and securely destroy the Employee's Personal Information in accordance with applicable laws and regulations.

Rights of Access, Correction, Erasure, and Objection

12. Employees must ensure that their Personal Information held by the College is accurate and current.
   12.1. Employees have the right to request access to and to correct their Personal Information held by the College, or to withdraw their consent to the use of their Personal Information under certain circumstances.
   12.2. If an Employee wants to review, verify, correct, or withdraw consent to the use of their Personal Information, they shall contact the Privacy Officer.
      12.2.1. Any such communication must be in writing.

13. The College may request specific information from an Employee to help confirm the Employee's identity and their right to access, and to provide the Employee with their Personal Information held by the College or make requested changes.
    13.1. Applicable law may allow or require the College to refuse to provide the Employee with access to some or all of the Personal Information held about them, or the College may have destroyed, erased, or made Personal Information anonymous in accordance with its record retention obligations and practices.
    13.2. If the College cannot provide the Employee with access to their Personal Information, the College will inform the Employee of the reasons why, subject to any legal or regulatory restrictions.

Privacy Officer

14. The Privacy Officer is responsible for overseeing compliance with this Policy. Any enquiries related to this policy or how Personal Information is handled shall be directed to the Privacy Officer.

RELATED DOCUMENTS

Policy Adm 1.0 – Confidentiality of College of Paramedics of Nova Scotia Information
Attachment A – Confidentiality Agreement

DOCUMENT HISTORY (Date of Reviews, revisions, etc):

Policy Name:	Responding to a Breach of Privacy		
Policy Number:	Administrative – 1.3		
Version Number:	1	**Date first Approved:**	09/28/2021
Approved by:	ED/Registrar	**Effective Date:**	09/28/2021
Version Date:	09/28/2021	**Next Review Date:**	MM/DD/YYYY

DEFINITIONS

"College" means the College of Paramedics of Nova Scotia.

"Council" means the Council of the College.

"Employee" has the meaning ascribed to it in the College's "Confidentiality of CPNS Information Policy".

"Personal Information" has the meaning ascribed to it in the College's "Privacy Policy".

"Privacy Breach" means any occurrence where there is confirmed inappropriate or unauthorized access to or collection, use, disclosure, or disposal of Personal Information, in contravention of applicable privacy legislation or the College's policies/procedures.

"Privacy Officer" means the Executive Director/Registrar of the College, or their designate;

"Third-Party Service Provider" has the meaning ascribed to it in the College's "Confidentiality of CPNS Information Policy".

"Volunteer" has the meaning ascribed to it in the College's "Confidentiality of CPNS Information Policy".

POLICY STATEMENT

1. Employees, Council members, Volunteers and Third-Party Service Providers of the College are to:
   1.1. Be knowledgeable on the procedures in place to prevent and manage Privacy Breaches.
   1.2. Ensure the College complies with all applicable privacy laws governing Personal Information in its custody or control.
   1.3. Demonstrate to stakeholders that a systematic procedure is in place to respond to and deal with a Privacy Breach.
   1.4. Encourage prompt identification, reporting, and resolution of Privacy Breaches.

2. This policy applies to:
   2.1. All Employees.

2.2. All Volunteers.
2.3. All Personal Information in the custody or control of the College.

PROCEDURE

1. The procedures below describe the approach the College will employ for managing an actual or suspected Privacy Breach.

2. The general order of events required to take place is as outlined below; however, tasks may occur in very quick succession or simultaneously.

Identification, Reporting and Documentation

3. The person who identifies an actual or suspected Privacy Breach shall immediately notify the Privacy Officer.
   3.1. The Privacy Officer will work with the individual who identified the Privacy Breach and document the Privacy Breach on the Privacy Breach Checklist attached as Attachment A.

Containment

4. The person who identified the actual or suspected Privacy Breach shall, in consultation with the Privacy Officer, take immediate and common-sense actions to contain the Privacy Breach by, for example:
   4.1. stopping the unauthorized practice;
   4.2. shutting down the system that was breached;
   4.3. recovering the Personal Information and all copies, ensuring no copies of Personal Information have been made or retained by the unauthorized person;
   4.4. revoking or changing computer access codes;
   4.5. sending a remote "kill" signal to a lost or stolen portable storage device;
   4.6. correcting weaknesses in physical security;
   4.7. notifying the police if a Privacy Breach appears to involve theft or other criminal activity; or
   4.8. searching the neighbourhood or used item websites (such as Kijiji) for items stolen containing the Personal Information.

5. The Privacy Officer will promptly ensure that all steps that are required to contain the Privacy Breach are taken, including any of the steps enumerated in 4 above.

6. The Privacy Officer, along with the person who identified the actual or suspected Privacy Breach, shall take all necessary actions to preserve any evidence associated with the Privacy Breach, including by being careful not to destroy evidence that may be valuable in determining the cause of the Privacy Breach or will allow the College to take appropriate corrective action.

Investigation and Risk Assessment

7. The Privacy Officer will investigate to understand and document the circumstances associated with the Privacy Breach and determine:
   7.1. What happened, when the Privacy Breach occurred (if known), who discovered it, when it was discovered, and how it was discovered;
   7.2. The nature and sensitivity of the Personal Information involved;
   7.3. The apparent cause of the Privacy Breach;
   7.4. The relationship between the recipient(s) of the information and the individual(s) affected by the Privacy Breach;
   7.5. The scope and extent of the Privacy Breach e.g., number of individuals affected, number of records involved, system(s) breached, the number of likely recipients of the Personal Information, the risk of further access, use or disclosure, including in mass media or online;
   7.6. The effectiveness of the containment efforts.

8. To understand the facts, the investigation may include steps such as:
   8.1. Interviewing individuals involved with the Privacy Breach or individuals who can provide information about the process and confirm details;
   8.2. Obtaining and reviewing relevant documentation;
   8.3. Observing, visiting, or inspecting the site of the Privacy Breach; and
   8.4. Consulting with external resources, such as legal advisors, security experts, and/or law enforcement officials, where and when appropriate.

9. The Privacy Officer will analyze the cause(s) and extent of the Privacy Breach to identify:
   9.1. System-induced causes (e.g., technical error, system compromise)
   9.2. Human causes (e.g., human error; theft; unauthorized access; loss);
   9.3. Whether the Privacy Breach can be attributed to a systemic (organizational) issue, gap or risk or to an isolated incident;
   9.4. Whether there is there a risk of ongoing or further exposure of the information.

10. Considering the circumstances, facts and cause(s) of the Privacy Breach, the Privacy Officer shall conduct a risk assessment, including whether the Privacy Breach poses a real risk of significant harm to the affected individual(s).

Assessment and/or Notification

11. The Privacy Officer shall review the risk assessment and consider the circumstances and facts of the Privacy Breach to determine whether individual(s) affected by the Privacy Breach should be notified. In making this determination, the Privacy Officer should consider:
    11.1. Whether there are any statutory, regulatory, or contractual notification requirements governing the College or which apply in connection with the Privacy Breach;

11.2. Whether there is a risk of identity theft or fraud;
11.3. Whether there is a risk of physical harm;
11.4. Whether there is a risk of hurt, humiliation, or damage to reputation;
11.5. Whether there is a risk of loss of business or employment opportunities;
11.6. Whether a risk of loss of confidence in the College and/or good citizen relations dictate that notification is appropriate.

12. If it is determined that individuals affected by the Privacy Breach should be notified, the Privacy Officer shall notify the affected individual(s) as soon as possible. Such notification should be provided directly, either by phone, letter, or in person, unless it is unreasonable or inappropriate to do so.
    12.1. To the extent reasonable and/or appropriate, the notification should include the following information:
        12.1.1. Date of the Privacy Breach;
        12.1.2. Description of the Privacy Breach;
        12.1.3. Description of the Personal Information inappropriately accessed, collected, used or disclosed;
        12.1.4. Risk(s) to the individual caused by the Privacy Breach;
        12.1.5. The steps taken so far to control or reduce the harm;
        12.1.6. Further steps planned to prevent future Privacy Breaches;
        12.1.7. Steps the individual can take to further mitigate the risk of harm;
        12.1.8. Contact information of the Privacy Officer who can answer questions or provide further information.

    12.2. The Privacy Officer shall review the risk assessment and consider the circumstances and facts of the Privacy Breach to determine whether any other authorities or organizations should be notified including the police, insurers, professional regulatory bodies, or other internal or external parties not already notified.

Prevention

13. The Privacy Officer shall consider the results of the investigation and the cause of the Privacy Breach for the purpose developing or improving preventative measures and safeguards to reduce the impact and likelihood of future Privacy Breaches.
    13.1. Preventative measures may include, for example:
        13.1.1. An audit of and improvements to physical safeguards (e.g. access to filing cabinets, office security, computer security);
        13.1.2. An audit of and improvements to technical safeguards (e.g. encryption, password protection);
        13.1.3. A review of training practices and recommendations to change or enhance training on specific topics;
        13.1.4. A review of policies and procedures and recommended revisions to reflect the lessons learned;
        13.1.5. A review of existing processes to determine if improvements are required;

13.1.6. Education of the Employees, Council members, Volunteers and Third-Party Service Providers of the College on how to avoid similar breaches;

13.1.7. Requiring individual(s) involved in the Privacy Breach to take additional privacy training to enhance the individuals' understanding of this policy, the College's privacy obligations, and how to reduce the risk of future Privacy Breaches.

Accountability

14. The Privacy Officer shall:
    - 14.1. Monitor and promote compliance with this policy;
    - 14.2. Review this policy on a regular basis to determine its effectiveness and recommend amendments if needed;
    - 14.3. Maintain procedures to support an effective response to any Privacy Breach;
    - 14.4. Ensure Privacy Breaches, related investigations, and resolutions are properly documented;
    - 14.5. Ensure Privacy Breaches are reported to the College's stakeholders when required in the circumstances, in a timely manner;
    - 14.6. Work collaboratively with stakeholders to resolve Privacy Breaches in a manner that minimizes risks to the College, its stakeholders and impacted individuals; and
    - 14.7. Identify preventative measures and monitor their completion.

15. Employees, Council members, Volunteers and Third-Party Service Providers of the College who handle Personal Information when carrying out their duties on behalf of the College are required to:
    - 15.1. Know, understand and comply with their obligations under this policy; and
    - 15.2. Immediately report any actual or suspected Privacy Breaches or privacy complaints to the Privacy Officer.

RELATED DOCUMENTS

Policy Adm 1.0 – Confidentiality of College of Paramedics of Nova Scotia Information,
Attachment A – Confidentiality Agreement
Policy Adm 1.3 - Responding to a Breach of Privacy, Attachment A - Privacy Breach Checklist

DOCUMENT HISTORY (Date of Reviews, Revisions, etc):

Attachment A

Privacy Breach Checklist

This checklist will be utilized to evaluate the College of Paramedics of Nova Scotia response to a Privacy Breach.

Date of report: _____

Date breach initially discovered: _____

Contact information:

Contact Person (Report Author): _____

Title: _____

Phone: _____

E-Mail: _____

Mailing Address: _____

Incident Description

Describe the nature of the breach and its cause. How was the breach discovered and when? Where did it occur?

_____

_____

_____

Steps 1 & 2: Containment & Risk Evaluation

Answer each of the following questions and then, based on those answers, complete the risk evaluation summary.

(1) Containment

Check all of the factors that apply:

- ☐ The personal information has been recovered and all copies are now in our custody and control.
- ☐ We have confirmation that no copies have been made.
- ☐ We have confirmation that the personal information has been destroyed.
- ☐ We believe (but do not have confirmation) that the personal information has been destroyed.
- ☐ The personal information is encrypted.
- ☐ The personal information was not encrypted.
- ☐ Evidence gathered so far suggests that the incident was likely a result of a systemic problem.
- ☐ Evidence gathered so far suggests that the incident was likely an isolated incident.

- ☐ The personal information has not been recovered but the following containment steps have been taken (check all that apply):
  - ☐ The immediate neighbourhood around the theft has been thoroughly searched.
  - ☐ Used item websites are being monitored but the item has not appeared so far.
  - ☐ Pawn shops are being monitored.
  - ☐ A remote wipe signal has been sent to the device but no confirmation that the signal was successful has been received
  - ☐ A remote wipe signal has been sent to the device and we have confirmation that the signal was successful.
  - ☐ Our audit confirms that no one has accessed the content of the portable storage device.
  - ☐ We do not have an audit that confirms that no one has accessed the content of the portable storage device.
  - ☐ All passwords and system usernames have been changed.

Describe any other containment strategies used:

_____

_____

_____

_____

_____

(2) Nature of Personal Information Involved

List all of the data elements involved (e.g. name, date of birth, SIN, address, medical diagnoses, connection with identified service provider such as welfare or counselling etc.)

- ☐ Name
- ☐ Address
- ☐ Date of birth
- ☐ Government ID number (specify) _____
- ☐ SIN
- ☐ Financial Information
- ☐ Medical information
- ☐ Personal characteristics such as race, religion, sexual orientation
- ☐ Other (describe)

_____

_____

_____

_____

(3) Relationship

What is the relationship between the recipient of the information and the individuals affected by the breach?

- ☐ Stranger
- ☐ Friend
- ☐ Neighbour
- ☐ Ex-partner
- ☐ Co-worker
- ☐ Unknown
- ☐ Other (describe)

_____

_____

_____

_____

(4) Cause of the Breach

Based on your initial investigation of the breach, what is your best initial evaluation of the cause of the breach?

- ☐ Accident or oversight
- ☐ Technical error
- ☐ Intentional theft or wrongdoing
- ☐ Unauthorized browsing
- ☐ Unknown
- ☐ Other (describe)

_____

_____

_____

(5) Scope of the Breach

How many people were affected by the breach?

- ☐ Very few (less than 10)
- ☐ Identified and limited group (>10 and <50)
- ☐ Large number of individuals affected (>50)
- ☐ Numbers are not known

(6) Foreseeable Harm

Identify the types of harm that may result from the breach. Some relate strictly to the affected individual, but harm may also be caused to the public body and other individuals if notifications do not occur:

- ☐ **Identify theft** (most likely when the breach includes loss of SIN, credit card numbers, driver's licence numbers, debit card information etc.)
- ☐ **Physical harm** (when the information places any individual at risk of physical harm from stalking or harassment)
- ☐ **Hurt, humiliation, damage to reputation** (associated with the loss of information such as mental health records, medical records, disciplinary records)
- ☐ **Loss of business or employment opportunities** (usually as a result of damage to reputation to an individual)
- ☐ **Breach of contractual obligations** (contractual provisions may require notification of third parties in the case of a data loss or privacy breach)
- ☐ **Future breaches due to technical failures** (notification to the manufacturer may be necessary if a recall is warranted and/or to prevent a future breach by other users)
- ☐ **Failure to meet professional standards or certification standards** (notification may be required to a professional regulatory body or certification authority)
- ☐ **Other** (specify)

_____

_____

(7) Other Factors

The nature of the College's relationship with the affected individuals may be such that the College wishes to notify no matter what the other factors are because of the importance of preserving trust in the relationship. Consider the type of individuals that were affected by the breach

- ☐ Client/customer/patient
- ☐ Employee
- ☐ Student or volunteer
- ☐ Other (describe)

  _____

Risk Evaluation Summary:

For each of the factors reviewed above, determine the risk rating.

Risk Factor	**Risk Rating**		
	Low	Medium	High
1) Containment			
2) Nature of the personal information			
3) Relationship			
4) Cause of the breach			
5) Scope of the breach			
6) Foreseeable harm from the breach			
7) Other factors			
Overall Risk Rating			

Use the risk rating to help decide whether notification is necessary and to design prevention strategies. Real risk of significant harm from the breach is usually the key factor used in deciding whether or not to notify affected individuals. Step 3 below analyzes this in more detail. In general, though, a medium or high risk rating will always result in notification to the affected individuals. A low-risk rating may also result in notification depending on the unique circumstances of each case.

Step 3: Notification

(1) Should Affected Individuals be Notified?

Once you have completed your overall risk rating determine whether or not notification of affected individuals is required. If any of the following factors apply, notification should occur.

Consideration	Description	Factor applies
Legislation	Health custodians in Nova Scotia must comply with sections 69 & 70 of PHIA which require notification.	
Risk of identity theft	Most likely when the breach includes loss of SIN, credit card number, driver's license number, debit card information, etc.	
Risk of physical Harm	When the information places any individual at risk of physical harm from stalking or harassment.	
Risk of hurt, humiliation, damage to reputation	Often associated with the loss of information such as mental health records, medical records or disciplinary records.	
Loss of business or employment opportunities	Where the breach could affect the business reputation of an individual.	
Explanation required	The public body may wish to notify if the affected individuals include vulnerable individuals, or where individuals require information to fully understand the events, even when the risks have been assessed as low.	
Reputation of public body	Where the public body is concerned that the breach will undermine trust of citizens, the public body may decide to notify in order to ease concerns and to provide clear information regarding the risks and mitigation strategies undertaken, even when risks assessed are low.	

(2) When and how to Notify

When: Notification should occur as soon as possible following a breach. However, if you have contacted law-enforcement authorities, you should determine from those authorities whether notification should be delayed in order not to impede a criminal investigation.

How: The preferred method is direct - by phone, letter, email or in person. Indirect notification via website information, posted notices or media should generally only occur where direct notification could cause further harm, is prohibitive in cost, or contact information is lacking. Using multiple methods of notification in certain cases may be the most effective approach.

Considerations Favouring Direct Notification	**Check If Applicable**
The identities of individuals are known	
Current contact information for the affected individuals is available	
Individuals affected by the breach require detailed information in order to properly protect themselves from the harm arising from the breach	
Individuals affected by the breach may have difficulty understanding an indirect notification (due to mental capacity, age, language, etc.)	
Considerations Favouring Indirect Notification	
A very large number of individuals are affected by the breach, such that direct notification could be impractical	
Direct notification could compound the harm to the individuals resulting from the breach	

(3) What to Include in Breach Notification Letters

The information included in the notice should help the individual to reduce or prevent the harm that could be caused by the breach. Include all of the information set out below:

Essential Elements in Breach Notification Letters	**Included**
Date of breach	
Description of breach	
Description of personal information affected	
Steps taken so far to control or reduce harm (containment)	
Future steps planned to prevent further privacy breaches	
Steps individuals can take	
Privacy Officer contact information - for further assistance	

Other Sources of Information

As noted above, the breach notification letter should include a contact number within the College of Paramedics of Nova Scotia, in case affected individuals have further questions. In anticipation of further calls, you should prepare a list of frequently asked questions and answers to assist staff responsible for responding to further inquiries.

Others to Contact

Regardless of what you determine your obligations to be with respect to notifying individuals, you should consider whether the following authorities or organizations should also be informed of the breach:

- Police - if theft or crime is suspected;
- Insurers or others - if required by contractual obligations;
- Professional or other regulatory bodies - if professional or regulatory standards require notification of these bodies;
- Other internal or external parties not already notified - your investigation and risk analysis may have identified other parties impacted by the breach such as third-party contractors, internal business units or unions.

Policy Name:	Security of Confidential Information of College of Paramedics of Nova Scotia		
Policy Number:	Administrative – 1.4		
Version Number:	1	**Date first Approved:**	19/10/2021
Approved by:	ED/Registrar	**Effective Date:**	19/10/2021
Version Date:	19/10/2021	**Next Review Date:**	MM/DD/YYYY

DEFINITIONS

"College" means the College of Paramedics of Nova Scotia.

"Confidential Information" has the meaning as described in the College's "Confidentiality of College of Paramedics of Nova Scotia Information"

"Council" means the Council of the College.

"Employee" has the meaning as described in the College's "Confidentiality of College of Paramedics of Nova Scotia Information"

"Personal Information" has the meaning ascribed to it in the College's "Privacy Policy".

"Third-Party Service Provider" has the meaning as described in the College's "Confidentiality of College of Paramedics of Nova Scotia Information"

"Volunteer" has the meaning as described in the College's "Confidentiality of College of Paramedics of Nova Scotia Information"

"Access Control" means the permissions assigned to persons or systems that are authorized to access specific resources.

POLICY STATEMENT

1. This policy applies to:
   1.1. All Employees;
   1.2. All Volunteers;
   1.3. All Third-Party Service Providers of the College;
   1.4. All Confidential Information of the College, or in its custody or control, in any form such as electronic and paper format.

2. The College will safeguard all confidential information within a secure environment.

3. All parties to whom this policy applies must:
   3.1. Protect information from unauthorized access or misuse.
   3.2. Ensure the confidentiality of information.
   3.3. Maintain the integrity of information.
   3.4. Maintain the availability of information systems and information for service delivery.
   3.5. Comply with regulatory, contractual, and legal requirements.
   3.6. Maintain physical, logical, environmental and communications security.
   3.7. Dispose of information in an appropriate and secure manner when it is no longer in use.

Authorized Users of Confidential Information

4. All users who have access to confidential information of the College must:
   4.1. Be formally authorized to do so by the Executive Director/Registrar of the College.
   4.2. Be in possession of a unique user identity when accessing any information systems of the College.
   4.3. Not disclose any password associated with their user identity to any person.
   4.4. Take all necessary precautions to protect the **confidential** information in their personal possession. Confidential information must not be copied or transported without consideration of:
      4.4.1. The permission to do so.
      4.4.2. The risks associated with loss or falling into the wrong hands.
      4.4.3. How the information will be secured during transport to its destination.

Acceptable Use of Information Systems

5. Users accounts on the College computer systems must only be used for the company's business and must not be used for personal activities during working hours.
   5.1. During breaks or mealtimes, limited personal use is permitted, but use must be legal, honest, and decent while considering the rights and sensitivities of others.
      5.1.1. Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to company systems for which they do not have authorization.
      5.1.2. Users shall not attach unauthorized devices on their PCs or workstations, unless they have received specific authorization from the Executive Director/Registrar, or their designee.
      5.1.3. Users shall not download unauthorized software from the Internet onto their PCs or workstations.

6. Unauthorized use of the company's computer system and facilities may constitute grounds for civil or criminal prosecution.

Access Control

7. The College will control access to confidential information resources that require protection against disclosure or modification.

8. Access controls will exist for all College information technology hardware and software resources, as well as paper files.

9. Users will be provided with controlled access only to the hardware, software, and paper files necessary for them to perform of their job requirements.

10. Only those who are authorized by the Executive Director/Registrar, or their designate, shall access password files on any network infrastructure component.
    - 10.1. Password files on servers will be monitored for access by unauthorized users.
    - 10.2. Copying, reading, deleting, or modifying a password file on any computer system is prohibited.

11. Users will not be allowed to logon as a System Administrator.
    - 11.1. Users who need this level of access to production systems must request access from the Executive Director/Registrar.

12. Users will be responsible for all transactions occurring during Logon sessions initiated by use of the user's password and ID.
    - 12.1. Users shall not logon to a computer and then allow another individual to use the computer or otherwise share access to the computer systems.

Handling Confidentiality of Information

13. All users who handle confidential information, regardless of the location from which they work, must:
    - 13.1. Store paper information in a locked filing cabinet or room accessible only to those who have a need to access the information.
    - 13.2. Protect electronic information via firewalls, encryption, and passwords.
    - 13.3. Clear their desks of any confidential information and secure any confidential information before going home at the end of the day, or when leaving their workspace unattended.
    - 13.4. Refrain from leaving confidential information visible on their computer monitors when they leave their workstations for any period of time.
    - 13.5. Ensure no unauthorized third-party gains access to the College's confidential information by never:
      - 13.5.1. Accessing information on an unauthorized third-parties IT system.
      - 13.5.2. Leaving unsecured hardcopies of documentation unattended at any time.

13.6. USB drives or external hard drives that contain confidential information are locked when not in use.
13.7. Mark as “confidential” written or electronic documents that contain confidential information.
13.8. Dispose of it properly by shredding or burning written documentation.
13.9. Refrain from discussing confidential information in public place
13.10. Use the College secure e-mail service to transmit it to other parties.
13.11. Before disposing of an old computer, use software programs to wipe out the data contained on the computer or have the hard drive destroyed.

Security of Confidential Information

14. All electronic information must:
    14.1. Be stored on the appropriate College computer systems.
    14.2. Regularly backed-up so that it can be restored if or when necessary.
    14.3. Disposed of in a secure manner.
    14.4. Not be placed on a CD or DVD at any time.
    14.5. Only be placed on a USB flash drive or external drive, when there is no other secure method of data transfer and only if the device is password protected and labelled appropriately as confidential.

User Responsibilities

15. Users are required to report any weaknesses, incidents of misuse or violations associated with in the security of the College’s confidential information.
16. Users must:
    16.1. Comply with security procedures and policies.
    16.2. Protect their user ID and passwords.
    16.3. Inform the Executive Director/Registrar, or their designate, of any security questions, issues, problems, or concerns.
    16.4. Assist the Executive Director/Registrar, or their designate, in solving security problems.
    16.5. Ensure that all IT systems supporting tasks are backed up in a manner that mitigates both the risk of loss and the costs of recovery.
    16.6. Be aware of the vulnerabilities of remote access and their obligation to report intrusions, misuse, or abuse to the Executive Director/Registrar, or their designate.
    16.7. Be aware of their obligations in the event that they store, secure, transmit and dispose of confidential information of the College.

College's Right to Monitor IT Hardware and Software

17. The College has the right and capability to monitor electronic information created and/or communicated by users using College hardware, software, and networks, including e-mail messages and usage of the Internet.
    17.1. It is not the College's policy or intent to continuously monitor all computer usage by users.
18. Users of the College's hardware, software, and networks, should be aware that the company may monitor usage, including, but not limited to:
    18.1. Patterns of usage of the Internet (e.g. site accessed, on-line length, time of day access), and users electronic files and messages to the extent necessary to ensure that the Internet and other electronic communications are being used in compliance with the law and with College policy.

RELATED DOCUMENTS

Adm 1.5 Cyber Security – Protecting College and Personal Devices

DOCUMENT HISTORY ((Date of Reviews. Revisions, etc):

Attachment A

Security Policies Agreement

I acknowledge that any violation of this agreement could cause harm to the College and frustrate the College's work. Therefore, as a signatory to this agreement I recognize that unauthorized use and disclosure of Confidential Information my lead to disciplinary action including immediate termination.

I will direct any questions regarding my confidentiality obligations to the Executive Director/Registrar. I have read and understand the above expectations within this agreement and more broadly within the Confidentiality and Privacy Policies of the College and agree to abide by this duty of confidentiality.

I acknowledge that I have received copies of the College of Paramedic of Nova Scotia security policies including:

Adm 1.4 – Security of Confidential of College of Paramedics of Nova Scotia Information
Adm 1.5 – Cyber Security – Protecting College and Personal Devices
Adm 1.6 – Acceptable Internet and Email Use of College Information Technology Systems

I have read and understand the policies. I understand that, if I violate any of these policies, I may be subject to disciplinary action, including termination.

I further understand that I will contact Executive Director/Registrar, if I have any questions about any aspect of these policies.

Signatory:

_____

Print Name

_____ _____

Signature *Date*

College Staff:

_____

Print Name

_____ _____

Signature *Date*

Policy Name:	Cyber Security – Protecting College and Personal Devices		
Policy Number:	Administrative – 1.5		
Version Number:	1	**Date first Approved:**	19/10/2021
Approved by:	ED/Registrar	**Effective Date:**	19/10/2021
Version Date:	19/10/2021	**Next Review Date:**	DD/MM/YYYY

DEFINITIONS

"College" means the College of Paramedics of Nova Scotia.

"Confidential Information" has the meaning as described in the College's "Confidentiality of College of Paramedics of Nova Scotia Information"

"Council" means the Council of the College.

"Employee" has the meaning as described in the College's "Confidentiality of College of Paramedics of Nova Scotia Information"

"Personal Information" has the meaning ascribed to it in the College's "Privacy Policy".

"Third-Party Service Provider" has the meaning as described in the College's "Confidentiality of College of Paramedics of Nova Scotia Information"

"Volunteer" has the meaning as described in the College's "Confidentiality of College of Paramedics of Nova Scotia Information"

POLICY STATEMENT

1. This policy applies to:
   1.1. All Employees;
   1.2. All Volunteers;
   1.3. All Third-Party Service Providers of the College;
   1.4. All Confidential Information of the College, or in its custody or control, in any form such as electronic and paper format.

2. All users are obligated to protect confidential information of the College.

Protect College and Personal Devices

3. Users are to keep both their College-issued and personal computer, tablet, and cell phone secure.

4. To keep devices secure users must, based upon the technology being utilized:
   4.1. Keep all devices password protected.
   4.2. Choose and upgrade a complete antivirus software.
   4.3. Do not leave devices exposed or unattended.
   4.4. Install security updates of browsers and systems monthly or as soon as updates are available.
   4.5. Log into company accounts and systems through secure and private networks only.

5. Users must avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

6. New users receiving company-issued equipment, will be provided with:
   6.1. Devices that have been set up by the IT company designated to support College operations.
   6.2. Instructions for password management.
   6.3. Instructions to protect their devices.

Email Security

7. To avoid virus infection or data theft, users must:
   7.1. Avoid opening attachments and clicking on links with:
      7.1.1. Content is not adequately explained (e.g. "Watch this video, it's amazing.")
      7.1.2. Clickbait titles (e.g. offering prizes, advice).
   7.2. Check email and names of people they received a message from to ensure they are legitimate.
   7.3. Look for inconsistencies or giveaways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks).

8. If a user is unsure that an email they received is safe, they must contact the Executive Director/Registrar, or their designate, for direction regarding the email.

Username and Password Identification

9. All users must have a unique username and password to access the Colleges IT infrastructure.
   9.1. Users password must remain confidential and under no circumstances should it be shared with management and supervisory staff and/or any other employees.
   9.2. Users must comply with the following rules regarding password creation and maintenance:
      9.2.1. Password must be at least eight characters (including capital and lower-case letters, numbers, and symbols) and avoid information that can be easily guessed (e.g. birthdays).
      9.2.2. Passwords should be remembered instead of writing them down.

9.2.2.1. If users need to write down their passwords, they are obligated to keep the paper or digital document confidential and destroy it when their work is done.

9.3. Password must be changed every 60 days;

9.4. User Logon IDs and passwords will be deactivated as soon as possible if the user is terminated, fired, suspended, placed on leave, or otherwise leaves the College.

9.5. Users who forget their Microsoft Office 365 password must call the Executive Director/Registrar, or their designate, to have their password reset.

Data Transfers

10. Users must:
    - 10.1. Avoid transferring confidential information to other devices or accounts unless absolutely necessary.
    - 10.2. When transferring confidential information use the College's secure email service, TitanFile.
    - 10.3. Ensure that the recipients of the data are properly authorized people or organizations.
    - 10.4. Report scams, privacy breaches and hacking attempts to the Executive Director/Registrar, or their designate.
    - 10.5. Contact the Executive Director/Registrar, or their designate, if they have any questions or concerns.

Additional Cyber Security Measures

11. To reduce the likelihood of security breaches, users must:
    - 11.1. Turn off their screens and lock their devices when leaving their desks.
    - 11.2. Report stolen or damaged equipment as soon as possible to the Executive Director/Registrar, or their designate.
    - 11.3. Change all account passwords at once when a device is stolen.
    - 11.4. Report a perceived threat or possible security weakness in company systems.
    - 11.5. Refrain from downloading suspicious, unauthorized, or illegal software on the College's equipment.
    - 11.6. Avoid accessing suspicious websites.

Remote Users

12. Remote users:
    - 12.1. Must follow the Cyber Security – Protecting College and Personal Devices Policy.
    - 12.2. Are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

13. Remote users must seek advice from the Executive Director/Registrar, or their designate.

RELATED DOCUMENTS

Policy Adm 1.4 Security of Confidential Information of College of Paramedics of Nova Scotia
Attachment A – Security Policies Agreement

DOCUMENT HISTORY ((Date of Reviews. Revisions, etc):

Policy Name:	Security – Acceptable Internet and Email Use of College Information Technology Systems		
Policy Number:	Administrative – 1.6		
Version Number:	1	**Date first Approved:**	19/10/2021
Approved by:	ED/Registrar	**Effective Date:**	19/10/2021
Version Date:	19/10/2021	**Next Review Date:**	MM/DD/YYYY

DEFINITIONS

"College" means the College of Paramedics of Nova Scotia.

"Confidential Information" has the meaning as described in the College's "Confidentiality of College of Paramedics of Nova Scotia Information"

"Council" means the Council of the College.

"Employee" has the meaning as described in the College's "Confidentiality of College of Paramedics of Nova Scotia Information"

"Personal Information" has the meaning ascribed to it in the College's "Privacy Policy".

"Third-Party Service Provider" has the meaning as described in the College's "Confidentiality of College of Paramedics of Nova Scotia Information"

"Volunteer" has the meaning as described in the College's "Confidentiality of College of Paramedics of Nova Scotia Information"

POLICY STATEMENT

1. This policy applies to:
   1.1. All Employees;
   1.2. All Volunteers and their internet access;
   1.3. All Third-Party Service Providers of the College and their internet access;
   1.4. All information technology equipment owned by the College including but not limited to all information technology and computer equipment (computers, printers, etc.), as well as use of email, the internet, Wi-Fi access points, voice, and mobile computing equipment.

2. Users must not:
   2.1. Use another users ID and password to access the College's IT systems.
   2.2. Perform any unauthorized changes to the College's IT systems or information.
   2.3. Attempt to access data that they are not authorized to use or access.

2.4. Connect any non-College authorized device to the College's network or IT systems.
2.5. Store data on any non-authorized equipment.
2.6. Give or transfer College data or software to any person or organization outside the College without the authority of the College.
2.7. The Executive Director/Registrar, or their designate, will ensure that users receive clear directions on the extent and limits of their authority over computer systems and data.

3. The Internet and email must be used for professional purposes.
3.1. Personal use is permitted provided it does not:
3.1.1. Affect the individual's professional performance.
3.1.2. In anyway harm the College.
3.1.3. Violate any terms and conditions of employment.
3.1.4. Place the user or the College in violation of legal or other obligations.

3.2. All users are responsible for their actions on the internet as well as when using email systems.

3.3. Users must not:
3.3.1. Use the internet or email for harassment or abuse.
3.3.2. Use obscenities or disrespectful remarks in communications.
3.3.3. Access, upload, send or receive data (including images) that the College considers offensive in any way, including sexually explicit, discriminatory, defamatory, or libellous material.
3.3.4. Use the College's resources to make personal gain or run a personal business.
3.3.5. Use the internet or email to play.
3.3.6. Use email systems in a way that could affect their reliability or efficiency, such as distributing chain letters or spam.
3.3.7. Open email attachments that are received from unknown senders, which may contain malware.
3.3.8. Remove or disable anti-virus software.
3.3.9. Place on the internet any information relating to the College, modify any information concerning it or express any opinion on the College, unless they are expressly authorized to do so.
3.3.10. Send sensitive or confidential information, via any means other than the College's secure email transfer system, TitanFile, unless permission to do so is first received from the Executive Director/Registrar, or their designate, and the information is protected.
3.3.11. Forward business email to personal email accounts (for example, Gmail account).
3.3.12. Make official commitments by internet or email on behalf of the College, unless authorized to do so.
3.3.13. Download copyrighted material such as music media files (MP3), films and videos (non-exhaustive list) without appropriate approval.
3.3.14. In any way, violate copyright, database rights, trademarks, or other intellectual property rights.

3.3.15. Download any software from the internet without the prior consent of the Executive Director/Registrar, or their designate.
3.3.16. Connect to a publicly accessible, non-secured internet connection.

4. Users shall only use software that is authorized by the College, on College computer systems.
   4.1. Authorized software must be used in accordance with the software supplier's licensing agreements.

5. Unacceptable email and internet use includes engaging in any activity that is illegal under local, provincial, federal, or international law.
   5.1. The following activities are strictly prohibited:
      5.1.1. Infringements of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or by similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" products or other software the use of which is not authorized by the College.
      5.1.2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the College or the end user holds no active license is strictly prohibited.
      5.1.3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal.
      5.1.4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
      5.1.5. Making fraudulent offers of services originating from any College account.
      5.1.6. Making security breaches or disruptions of network communication.
      5.1.7. Executing any form of network monitoring which will intercept data not intended for the user's host unless this activity is a part of the employee's normal job/duty.
      5.1.8. Circumventing user authentication or security of any host, network, or account.
      5.1.9. Interfering with or denying service to any user other than the user's host (for example, denial of service attack).
      5.1.10. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

RELATED DOCUMENTS
Policy Adm 1.4 Security of Confidential Information of College of Paramedics of Nova Scotia
Attachment A – Security Policies Agreement

DOCUMENT HISTORY ((Date of Reviews. Revisions, etc):

Policy Name:	Conflict of Interest Policy		
Policy Number:	Administrative – 1.7		
Version Number:	1	**Date first Approved:**	04/28/2023
Approved by:	ED/Registrar	**Effective Date:**	04/28/2023
Version Date:	04/28/2023	**Next Review Date:**	MM/DD/YYYY

DEFINITIONS

"Applicable Persons" means Councillor members, Committee members, volunteers, employees, and third-party service providers.

"Actual conflict of interest" means a situation where an Applicable Person has a private or personal interest that is sufficiently connected to their College duties and responsibilities that it influences the exercise of these duties and responsibilities.

"Perceived conflict of interest" means a situation where reasonably well-informed persons could properly have a reasonable belief that an Applicable Person has an actual conflict of interest, even if they do not.

"Potential conflict of interest" means a situation where an Applicable Person has a private or personal interest that could influence the performance of their College duties or responsibilities, provided that they have not yet exercised that duty or responsibility.

POLICY STATEMENT

1. The College shall conduct all its affairs with integrity and independence. Conflicts of interests, whether actual, perceived, or potential, must not undermined these values.

2. The policy applies to all Applicable Persons with respect to the affairs of the College and their College duties and/or responsibilities.

3. This policy does not apply where an Applicable Persons interest is so remote or insignificant that it cannot reasonably be regarded as likely to influence the Applicable Person or where a pecuniary or other interest is in common with a board group of which the Applicable Person is a member.

4. Applicable Persons must use this policy to recognize, disclose, manage and resolve actual, perceived, and potential conflict of interests.

5. Applicable Persons must act in ways that preserve and enhance the reputation and integrity of the College.

6. Applicable Persons must perform their College duties with the best interests of the College in mind and put the best interests of the College first.

7. Applicable Persons who hold an outside office or employment should not place themselves in a conflict-of-interest situation or in a position which raises doubts about their capacity to perform their College duties in an objective manner.

8. Applicable Persons are required to disclose to the College any personal, business, commercial, financial, or other interest which could be construed to be an actual, perceived, or potential conflict of interest.

9. Applicable Persons must not permit their own interests to interfere with any decisions they may make, or have influence over, regarding the business and operations of the College or decisions made on behalf of the College.

10. Unless authorized to do so by the College in writing, an Applicable Person may not:
    10.1. act on behalf of the College, or deal with the College, in any matter where they are in a conflict of interest or appear to be in a conflict of interest; or
    10.2. use their position with the College to pursue or advance their personal interests or the interests of a person they are closely associated.

11. An Applicable Person must not use their relationship with the College to confer a benefit to:
    11.1. another Applicable Person;
    11.2. a close friend, family member, business associate of an Applicable Person;
    11.3. a corporation or partnership in which a Councillor or an Applicable Person a significant interest; and/or
    11.4. a person to whom an Applicable Person owes an obligation.

12. If a conflict of interest arises between the private interests of an Applicable Person and the College duties of that individual, the conflict shall be resolved in favour of the College.

PROCEDURE

1. All Applicable Persons new to the College shall review and sign the Conflict-of-Interest Agreement **(See Attachment A)** prior carrying out any College duties or responsibilities.

2. All Applicable Persons shall review the Conflict-of-Interest Policy of the College prior to attending a meeting, so they knowledge of the policy prior to the meeting.

2.1. When the Chair asks for conflicts of interest at the beginning of a meeting, all Applicable Persons will respond appropriately according to their circumstances.

3. At the beginning of every meeting, the Chair of the Council or Committee, as applicable, shall ask and have recorded in the minutes whether any Applicable Person has a conflict to declare in respect to any agenda item.
   3.1. Notwithstanding the above statement, all parties in a matter before the Council or a Committee of the College may be screened for conflicts of interest prior to a meeting.

4. In the event of an actual, perceived, or potential conflict of interest, the Applicable Person shall be recused from the meeting for the duration of the discussion and not participate in any the vote on the matter.
   4.1. The minutes are to record that the Applicable Person(s) in conflict of interest were recused from the discussion and did not vote on the matter.

Recognizing and Disclosing Conflicts

5. An Applicable Person is presumed to have become aware of a conflict of interest at such a time as a reasonable person would have been aware of it.

6. In cases where a conflict cannot be avoided, an Applicable Person must declare a conflict of interest at the earliest opportunity and, at the same time, should declare the general nature of the conflict.

7. If an Applicable Person is uncertain whether they are in conflict of interest, they must raise the perceived potential conflict with the Council or Committee, as applicable, and the Council or Committee is to determine whether or not a conflict of interest exists.
   7.1. If discussions do not lead to a resolution, whether or not a conflict exists is to be determined by majority vote.
      7.1.1. The Applicable Person perceived to be in conflict is to refrain from voting.

8. Where a conflict of interest is discovered after consideration or decision of a matter, it is to be declared to the Council or Committee, as applicable, and appropriately recorded at the first opportunity.
   8.1. If the Council or Committee determines that the involvement of the Applicable Person influenced the decision of the matter, the Council or Committee may re-examine the matter and may rescind, vary, or confirm its decision.

9. Any Applicable Person who perceives another Applicable Person to be in conflict of interest in a matter under consideration is to raise this concern with the Council or Committee, as applicable. If discussions do not lead to a resolution, whether or not a conflict exists is to be determined by majority vote.

9.1. The Applicable Person perceived to be in conflict is to refrain from voting.

Rules About Gifts

10. An Applicable Person may only accept a gift made to them because of their involvement in the College in the following circumstances:
    10.1. the gift has no more than token value;
    10.2. it is the normal exchange of hospitality or a customary gesture of courtesy between persons doing business together;
    10.3. the exchange is lawful and in accordance with local ethical practice and standards; and
    10.4. the gift could not be construed by an impartial observer as a bribe, pay off or improper or illegal payment.

11. An Applicable Person may not use the College's property to make a gift, charitable donation or political contribution to anyone on behalf of the College.
    11.1. Any gift must have the authorization of the College or a person the College designates.

12. If the acceptance of any gift might give rise to criticism or concern about a conflict of interest, it should be politely declined.

RELATED DOCUMENTS
Attachment A – Examples of Conflicts of Interest
Attachment B – Conflict of Interest Agreement

DOCUMENT HISTORY (Date of Reviews, Revisions, etc):

Attachment A

Examples of Conflicts of interest

When assessing for conflicts of interest one must recognize that there are different types of interests that may create a conflict. Additionally, conflicts of interest may appear in one of three different forms.

The types of interests a decision-maker must be aware of are:

- Individual/personal.
- Client.
- Professional.
- Employer.
- Organizational.
- Public.
- Owner.
- Recipients of Paramedic Services.
- Any other entities where a person may have interests.

Conflicts of interest may come in three different forms including:

- Actual
- Potential, and
- Perceived.

Avoiding actual, potential, and perceived conflicts of interest are fundamental to ensuring the highest level of integrity and public trust.

Potential Conflicts of Interest can arise from situations where a decision-maker:

- Knows a party to the decision or their family on a personal level.
- Is currently teaching, or has previously taught, a party to the decision, or vice versa.
- Is currently supervising, or has previously supervised, a party to the decision, or vice versa.
- Works closely with a party to the decision within another context, such as committee work, or another organization.
- Has a financial obligation to a party to the decision or anyone associated with a party to the decision.

Attachment B

Conflict of Interest Agreement

This Confidentiality Agreement is entered into, by the signatory, on the below date. This agreement applies to all Applicable Parties as described in the College's Conflict of Interest Policy.

I have read and been provided with the opportunity to obtain additional information regarding the College's policy on conflicts of interest.

I understand that as a signatory to this agreement that:

- I have a duty to not use my position with the College for any improper purpose.
- I undertake to avoid all situations in which my personal or business interests' conflict, might conflict or are perceived to conflict with my duties to the College.
- I shall declare and remove myself from both the discussion and vote on any matter where I am in an actual, perceived, or potential conflict of interest.
- In the event, that I am in a conflict-of-interest situation, the conflict and my name will be recorded in the Minutes.
- I undertake not to accept gifts, other than that described in policy, from current or prospective clients or suppliers.

I acknowledge that any violation of this agreement could cause harm to the College and frustrate the College's work. Therefore, as a signatory to this agreement I recognize that failing to disclose conflicts of interest may lead to disciplinary action including immediate termination.

By signing this document, I have read and understand the above expectations within this agreement and more broadly within the Conflict-of-Interest Policy of the College and agree to abide by its terms.

Signatory: _____

Print Name

_____ _____

Signature *Date*

College Staff: _____

Print Name

_____ _____

Signature *Date*