



COLLEGE OF THE NORTH ATLANTIC

OPERATIONAL PROCEDURE

TOPIC: PRIVACY BREACH

Procedure No.	PA-602-PR	Division	Public Affairs
Supersedes	n/a	Board Policy Ref.	GP-GR-807 & GP-RR-904
Related Policy	PA-602	Effective Date:	February 18, 2022

PROCEDURE

1.0 Legislative Context

This procedure is aligned with the requirements of the privacy legislation that applies to College of the North Atlantic (CNA). The [Access to Information and Protection of Privacy \(ATIPP\) Act, 2015](#) of Newfoundland and Labrador is the primary privacy legislation with which CNA shall comply.

Definitions

Access and Privacy Office	The CNA unit responsible for administering the Management of Information Act, and the Access to Information and Protection of Privacy Act, 2015 for CNA.
Employee	A person retained under a contract to perform services for CNA.
Personal Information	Information about an identifiable individual.
Privacy Breach	A privacy breach occurs when there is unauthorized and/or inappropriate access to the collection, use, disclosure or disposal of personal information. A privacy breach can occur without the existence of a record.

Record Information in any form, and includes a dataset, information that is machine readable, written, photographed, recorded or stored in any manner, but does not include a computer program or a mechanism that produced records on any storage medium.

3.0 Roles and Responsibilities

3.1 All employees are responsible to:

- A. Protect personal information to which you have access to from unauthorized access, collection, use or disclosure.
- B. Immediately report any suspected or confirmed privacy breach to the relevant supervisor/manager and to the Access and Privacy Office (APO).
- C. Assist in the containment of the suspected or confirmed privacy breach, where possible.

3.2 Supervisor and/or Department heads are responsible to:

- A. Provide access to personal information for employees only as it is required to fulfill their CNA job duties or responsibilities.
- B. Promote awareness among employees of CNA policies, procedures, and legal responsibilities under the *ATIPP* Act, 2015 for responding to a suspected or confirmed privacy breach.
- C. Appropriately contain the suspected or confirmed privacy breach.
- D. Assist the APO to contain all the relevant information about the nature of the potential or confirmed breach.
- E. Work with the APO to identify root causes and any response actions required to prevent any future privacy breaches.
- F. Implement any approved response actions, where identified in an effective manner and timely manner.

3.3 CNA's APO will be responsible to:

- A. Coordinate the investigation and response to a potential or confirmed privacy breach.
- B. Brief the Executive team on the potential or confirmed privacy breach as necessary.

- C. Notify the appropriate government agencies of the confirmed privacy breach.
 - D. Where deemed appropriate, notify those individuals whose personal information has been breached.
 - E. Maintain the official CNA records related to a privacy breach in accordance with an approved records retention and disposal schedule.
 - F. Monitor and report on the status of the implementation of any identified response actions.
 - G. Provide privacy breach training to employees.
 - H. Review and update CNA privacy breach policies and procedures on a regular basis.
- 3.4 Executive members will be responsible to:
- A. Establish, implement, review, and continually improve operational procedures to:
 - Secure and protect personal information in accordance with the *ATIPP Act, 2015* for CNA.
 - Establish and implement systematic access, maintenance and appropriate disposal of CNA records, in accordance with an approved Records Retention and Disposal Schedule (RRDS).
- 3.5 The Associate Vice-President of Public Affairs and the APO have been delegated the primary responsibility for administering the *ATIPP Act, 2015* for CNA.
- 3.6 The President is accountable for ensuring that CNA is compliant with the *ATIPP Act, 2015*.

4.0 Related Policies and Procedures

- 4.1 Access to Information Request; PA-601
- 4.2 Student Records; SS-206 & SS-206-PR
- 4.3 Electronic Information System Use; IS-501 & IS-501-PR
- 4.4 Electronic Mail (Email) and Internet Usage; IS-502 & IS-502-PR
- 4.5 Personal & Confidential College Data Encryption; IS-503 & IS-503-PR
- 4.6 Mobile Computing Devices Procurement & Use; IS-504 & IS-504-PR
- 4.7 Network User Accounts; IS-505 & IS-505-PR

4.8 Board Policy Access to Information; GP-GR-807

5.0 Appendices

5.1 Appendix A – *Government Privacy Breach Reporting Form*

5.2 Appendix B – FYI - *Privacy Breach*

Approval History	
Approved by President	April 19, 2012
Revision 1	April 28, 2016
Revision 2	November 4, 2016
Revision 3	November 18, 2022