CONESTOGA
Connect Life and Learning

PRIVACY BREACH PROCEDURE

Authorizer: Vice President, Finance and Corporate Services

Version: V1

Effective Date: September 4 2019

PROCEDURE STATEMENT:
In the event of a breach of security safeguards, the following procedure must be implemented immediately, in order to contain the breach and take any necessary corrective action.

DEFINITIONS:

Breach of security safeguards:

- The loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of security safeguards or from a failure to establish safeguards.

FIPPA:

- The Freedom of Information and Protection of Privacy Act (FIPPA)

Personal information:

- Information about an identifiable individual

PHIPA:

- The Personal Health Information Protection Act (PHIPA)

PROCEDURE:

1. **Report**
   a. Any employee or other person working for the college who becomes aware of a possible breach will immediately inform the Access and Privacy Coordinator (Corporate Services). Call or e-mail privacy@conestogac.on.ca without disclosing the potential breach to others.
   b. The individual reporting the breach will provide the Access and Privacy Coordinator with the basic facts:
      i. What happened?
      ii. When?
      iii. Who is involved?

iv. What information is potentially affected?

2. Contain

a. The Access and Privacy Coordinator, working with the relevant department(s), information technology staff and others as appropriate, will:
   i. Conduct an initial assessment and, if the report raises a valid concern, promptly take reasonable steps to prevent further disclosure of or compromise to personal information (e.g. re-set passwords, repair vulnerability) with a view to preserving all evidence that may show the scope of the breach.
   ii. Take all reasonable steps to retrieve and secure any records of personal information that can be readily retrieved.

3. Investigate

a. The Access and Privacy Coordinator, in consultation with executive staff, legal counsel and human resources staff as required, will:
   i. Take all reasonable steps to confirm that the breach has been contained.
   ii. Take all reasonable steps to determine the scope and potential consequences of the breach. What information was likely compromised? Who was likely affected?
   iii. Take all reasonable steps to determine the cause of the breach.

4. Mitigate

a. Departments involved in the breach, with guidance from the Access and Privacy Coordinator, will take all reasonable steps to mitigate the consequences or potential harm that the breach may cause. The Access and Privacy Coordinator will consult with executive staff and legal counsel as needed in order to provide guidance as the following items are considered:
   i. Notification issues:
      (1) Is notification to affected individuals required or otherwise appropriate? Do affected individuals need to know so they can protect themselves? Are affected individuals likely to find out anyway? Will notification simply cause unnecessary distress?
      (2) Is it appropriate to notify others who can help? The police? Financial institutions?
      (3) Is notification of the Information and Privacy Commissioner (IPC) required or otherwise appropriate? Does PHIPA's mandatory notification duty apply? Are affected individuals likely to contact the IPC anyway?
   ii. Clear, consistent messaging and strong support:
      (1) Consider what all affected individuals and the public should know.
      (2) Consider how to deliver messages. Phone, in person, in writing? Media release?
      (3) Anticipate other questions and prepare concise answers.
      (4) Consider who will answer questions and how.

5. Remedy

a. The relevant department(s), in consultation with the Access and Privacy Coordinator,

will commit to reasonable action for protecting against a recurrence, considering administrative measures (e.g. policy, procedure, training), technical measures and physical measures. This will include consideration of who will take the measures and what timeframe will be adhered to.

b. The relevant department(s), in consultation with the Access and Privacy Coordinator, will reflect on the incident response process to identify and commit to process improvement.

6. Close

a. The relevant department(s), in consultation with the Access and Privacy Coordinator, will conclude the procedure when reasonable steps to understand the scope and cause have been taken, reasonable steps to mitigate the consequences have been taken and a remedial plan has been developed.

b. The Access and Privacy Coordinator will record what was done at each step in the procedure, ensuring that only facts are recorded.

REFERENCES:

Freedom of Information and Protection of Privacy Act (FIPPA)
Personal Health Information Protection Act (PHIPA)
Protection of Student Privacy Policy

REVISION LOG:

Academic Forum	3/4/2019
Academic Coordinating Committee	9/4/2019