Privacy Breach Protocol

Nova Scotia Department of Education and Early Childhood Development

Purpose

The purpose of this protocol is to outline the steps that must be followed when the Department of Education and Early Childhood Development learns of a possible breach of personal privacy. It will assist the Department in controlling the situation and ensuring that, if a breach of privacy occurs, steps will be taken to prevent a similar breach from happening again.

Scope

This protocol applies to employees of the Department of Education and Early Childhood Development, and volunteers, students, and interns.

Background

A privacy breach occurs when personal information is collected, retained, used, disclosed or disposed of in ways that do not comply with the provisions of the Freedom of Information and Protection of Privacy Act. The most common breach of personal privacy is the loss or unauthorized disclosure of personal information, for example through theft of a computer or handheld electronic device, or because an email was sent to a wrong address.

How to Respond to a Breach or Suspicion of Breach

1. Identify the privacy beach

Identify and record the date, time, location, length, type and extent of breach.

2. Take immediate remedial action

Identify what action is necessary to contain or stop the breach. For example:

- Retrieve hard copies of personal information, or if that is not practical, the recipient(s) must confirm that the hard copies were securely disposed.
- Recall unopened Outlook email. For email that has been opened, request the email be deleted and hard copies be securely destroyed.
- For recipient(s) not on Outlook, contact the recipient(s) to request deletion of the email and secure disposal of any hard copies.
- Request that electronic copies of any personal information that has been disclosed be deleted from the individual's desktop computer, server, and any other storage device or media.
- Determine whether the breach will allow access to any other personal information, and if so, take steps to avoid this potential additional breach.
- Determine whether the breach will allow unauthorized access to any other personal information (e.g., an electronic information system). Take whatever necessary steps are appropriate (e.g., change passwords, identification numbers and/or temporarily shut down a system).
- If an electronic device and paper records containing personal information was stolen, contact security (if

within a Department of Education and Early Childhood Development facility) and/or the police (if outside the Department's facilities).

3. Internal notification

The individual who suspects a breach must notify their manager and the Manager, Information Management Division. The Manager, Information Management Division, will:

- contact the Director, Information Technology if the breach involves a website
- contact the Chief, Information Office if there is a danger to an individual or the public
- contact the Deputy Minister and Legal Counsel if the breach is serious or has the potential to be serious
- contact the Communications Director if the breach is or will be a matter of public interest.

4. Investigation and documentation

Determine the detail of what and whose personal information is involved, and what the extent/scope of the breach is. Sample questions:

- Were the immediate remedial actions effective?
- Is there enough documented evidence about the incident to determine the series of events that lead to the breach?

5. External notification

When personal privacy is breached, it is necessary to determine what stakeholders (e.g. public bodies or municipalities, general public, individuals etc.) should be notified, under what circumstances, and when.

After the Manager, Information Management Division, consults with the Deputy Minister (Head) and Legal Counsel, one or more of the following may need to be notified:

- Individual(s) whose privacy has been breached;
- Deputy Minister of NS Economic Development (Chair of BTAC);
- Communications Nova Scotia (through the Department's Communications Director);
- Security Authority or Deputy Minister of Transportation and Infrastructure Renewal
- Other individuals who may have been affected by the breach

6. Follow-up and long term remedial action

Determine what follow-up and long-term remedial action there will be to prevent the breach from occurring again, e.g. report with analysis and listing of future preventive measures. Example questions include:

- Was the privacy breach protocol followed?
- Are new or amended policies, procedures and/or training required to prevent reoccurrence of the breach?
- What plans have to be developed to lessen the likelihood or eliminate the possibility of another breach?