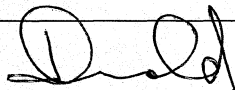


PRIVACY BREACH MANAGEMENT POLICY

DM Approval:



Effective Date: September 1, 2016

GENERAL INFORMATION

Under the *Access to Information and Protection of Privacy Act (ATIPP Act)* public bodies such as the Department of Education are accountable for protecting the personal privacy of individuals by preventing the unauthorized use or disclosure of personal information that it collects.

As a public body the Department of Education must make reasonable security arrangements against risks such as accidental loss and unauthorized access to and use, disclosure, or disposal of personal information.

Privacy breaches can occur when a person's personal information is collected or used by someone who does not have the authority to collect or use it, or when personal information is mistakenly disclosed, lost, or stolen.

This policy is part of the Department of Education's Privacy Management Program.

PURPOSE

The purpose of this policy is to establish a process for Department of Education staff to follow when there is an unauthorized use or disclosure of personal information within Yukon Education.

DEFINITIONS

'Personal Information', as defined under the *ATIPP Act*, means recorded information about an identifiable individual including:

- the individual's name, address, or telephone number;
- the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations;
- the individual's age, sex, sexual orientation, marital status, or family status;
- an identifying number, symbol, or other particular assigned to the individual;
- the individual's fingerprints, blood type, or inheritable characteristics;
- information about the individual's health care history, including a physical or mental disability;

- information about the individual's educational, financial, criminal, or employment history;
- anyone else's opinions about the individual; and
- the individual's personal views or opinions, except if they are about someone else.

'Privacy Breach' means the unauthorized collection of personal information or the unauthorized access to or use, disclosure, or disposal of personal information.

'Record' as defined under *ATIPP* includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other things on which information is recorded or stored by graphic, electronic, mechanical or other means.

POLICY STATEMENT

All privacy breaches will be managed in an effective and timely manner, recognizing that privacy breaches may require different levels of resources and expertise according to the nature, size, or complexity of the breach.

Those designated with responsibility for managing privacy breaches within the department will be provided with appropriate training to ensure the effective management of all privacy breaches, including the need to access additional expertise when necessary.

Factors to Consider When Investigating and Managing Privacy Breaches

The following factors must be considered when investigating and managing a privacy breach:

1. The sensitivity of the personal information (for example, whether the personal information can be easily obtained using other means, such as a phone book - if so, it is not sensitive information). The more sensitive the personal information is, the higher the risk of harm to the person. Some personal information can lead to identity theft and is more sensitive than others (for example, health information, social insurance and health care numbers, and financial account numbers such as credit card numbers). The sensitivity of the personal information alone is not the only criterion to use in assessing the risk resulting from the privacy breach - foreseeable harm to individuals is also an important factor to be considered.
2. The amount of personal information that was disclosed, and whether the privacy breach was an isolated incident or an example of a more systemic problem.
3. The number and nature of the individuals who received the personal information, and the risk of further unauthorized access, use or disclosure of the information.
4. Whether there is any relationship between the person and the recipients of the personal information (for example, was the disclosure to an unknown party or to a

party suspected of being involved in criminal activity where there is a potential risk of misuse? Alternatively, was the recipient a known and trusted person who could reasonably be expected to return the information without disclosing or using it?).

5. Whether the personal information can be used for fraudulent or otherwise harmful purposes including security risks, identity theft, loss of business or employment opportunities, or humiliation and damage to a person's reputation or relationships. The combination of certain types of sensitive personal information along with the person's name, address and date of birth results in a higher risk due to the potential for identity theft.
6. The risk of harm to the individual whose personal information was disclosed, including physical harm (for example, does the loss put an individual at risk of physical harm, stalking or harassment?)
7. Whether there is a risk of humiliation or damage to a person's reputation (for example, personal information about the person's mental health, or medical or disciplinary records).
8. Whether the personal information or record was adequately encrypted, anonymous or was otherwise not easily accessible.
9. Whether the personal information was lost or stolen - if it was stolen, whether it was the personal information that was the target of the theft.
10. Whether the personal information or record has been recovered, and whether it was copied.
11. The steps already taken to mitigate the effects of the privacy breach.
12. Whether harm such as risk to public health or risk to public safety could result from the privacy breach.
13. Whether harm such as loss of trust in the public body, loss of assets, financial exposure or legal proceedings could result from the privacy breach.
14. Whether there are applicable legal and contractual requirements to notify an individual that the privacy breach has occurred.

Process for Investigating and Managing Privacy Breaches

The attached 'Privacy Breach Checklist' should be used to assist the process of investigating and managing the effects of a privacy breach (see Appendix 'A').

The following steps must be taken when a privacy breach occurs within the Department of Education.

Step 1 - Containment of the Privacy Breach

The following actions must be taken to contain the effects of any privacy breach:

1. The Department of Education's ATIPP Coordinator must be notified, and a preliminary assessment of the breach must be conducted. The ATIPP Coordinator will assist in identifying the appropriate Department of Education staff to respond to the privacy breach, including conducting any investigation.
2. The personal information or record that was disclosed must be identified and recovered (if possible), including any copies of the personal information or record that were made as a result of the privacy breach.
3. Any practice or procedure that led to the privacy breach must be identified and immediately discontinued, any system that may have been breached must be shut down, and passwords or other computer access codes must be revoked or changed as required.
4. Any other breaches of physical or electronic security must also be identified and corrected.
5. The persons to be notified of the privacy breach must be identified.
6. If the privacy breach involves theft or any other criminal activity, the police must be notified and action should immediately be taken to ensure that any police investigation will not be compromised.

Step 2 – Notification

Persons affected by the privacy breach must be notified of the breach so that they can take steps to mitigate the effects of the breach and protect their personal information.

When Notification Should Occur

Persons affected by the privacy breach should be notified as soon as reasonably possible following the initial assessment and evaluation of the privacy breach.

If the police are involved, they should be consulted about the timing of any notification to ensure that the police investigation is not compromised.

How Notification Should Occur

Persons affected by a privacy breach should be notified directly – in person, by phone, or by letter or e-mail. Whenever possible, individuals should be notified in person or by phone and then be provided with written notification.

Indirect notification (e.g. website information, posted notices etc.) should only be used when direct notification would cause additional harm, the cost of direct notification is prohibitive, or the contact information of affected persons is unknown.

Notification of persons affected by a privacy breach should normally be done by a person from the work unit in which the breach occurred. There may be circumstances in which notification by a third party is more appropriate, such as where doing so will reduce the risk of additional harm to the person affected by the privacy breach.

Content of the Notification

It is important to ensure that the notification of a privacy breach does not contain unnecessary personal information, in order to avoid any further unauthorized disclosure of personal information.

The notification of a privacy breach should normally include the following information:

- Information about the privacy breach in general terms.
- A description of the personal information or record involved.
- A general account of what the Department of Education has already done to control or reduce the harm arising from the breach.
- An indication of what the Department of Education will do to assist the person, and what steps they can take to avoid or reduce the risk of harm resulting from the privacy breach (for example, arranging for credit monitoring or other fraud prevention tools, providing information on how to change a social insurance number, personal health card or driver's licence number).
- Sources of information designed to assist those affected to protect themselves against identity theft.
- Contact information for the Yukon Education ATIPP Coordinator and other Department of Education staff who can answer questions or provide further information and assistance.
- Contact information for the Information & Privacy Commission.

Other Persons Who May Require Notification

Depending on the circumstances of the privacy breach it may be appropriate to notify other persons of the breach, including:

- The police, if theft or other criminal activity is known or suspected.
- Insurers or others, if notification is required by contractual obligations.
- Professional or other regulatory bodies if professional or regulatory standards require notification of those bodies.
- Credit card companies, financial institutions or credit reporting agencies if their assistance is necessary for contacting individuals or assisting with mitigating harm arising from the privacy breach.
- Third party contractors or other parties who may be affected by the privacy breach.
- Other Department of Education or government units not previously advised of the privacy breach (for example, communications and media relations, senior management) or other bodies such as bargaining agents.

Step 3 – Identify and Implement Prevention Measures

Once the immediate steps are taken to mitigate the risks associated with the privacy breach it is necessary to identify and implement measures to help ensure that similar privacy breaches do not occur in the future.

The following actions should be considered in identifying the appropriate prevention measures to implement:

- A security audit of both physical and technical security.
- The need to review and amend this policy and/or to develop additional policies and procedures under the Department of Education Privacy Management Program.
- A review of employee training practices and the need for additional training.

ROLES AND RESPONSIBILITIES

The Deputy Minister is responsible for ensuring that Department of Education staff are aware of and meet their responsibilities under the *ATIPP Act*, and for ensuring that sufficient resources and support are available to meet the requirements of this policy.

The Director of Privacy and Risk Management Programs and the ATIPP Coordinator are responsible for coordinating and providing assistance to Department of Education staff in the investigation and management of privacy breaches within the department.

All Department of Education staff are responsible for following this policy and for managing privacy breaches that occur within the department in accordance with the requirements of this policy.

APPLICATION

This policy applies to all staff of the Department of Education.

EXCEPTIONAL CIRCUMSTANCES

In situations where the individual circumstances of a case are such that the provisions of this policy cannot be applied or to do so would result in an unfair or an unintended result, the decision may be based on the individual merits and justice of the situation. Such a decision will be considered for that specific case only and will not be precedent setting.

EFFECTIVE DATE

This policy is effective September 1, 2016.

LEGISLATIVE AND POLICY REFERENCES

Access to Information and Protection of Privacy Act, Part 3.

G.A.M. Policy 2.24 'Access to Information and Protection of Privacy Roles and Responsibilities'.

HISTORY

Privacy Breach Management Policy, effective October 1, 2014; revised effective September 1, 2016.