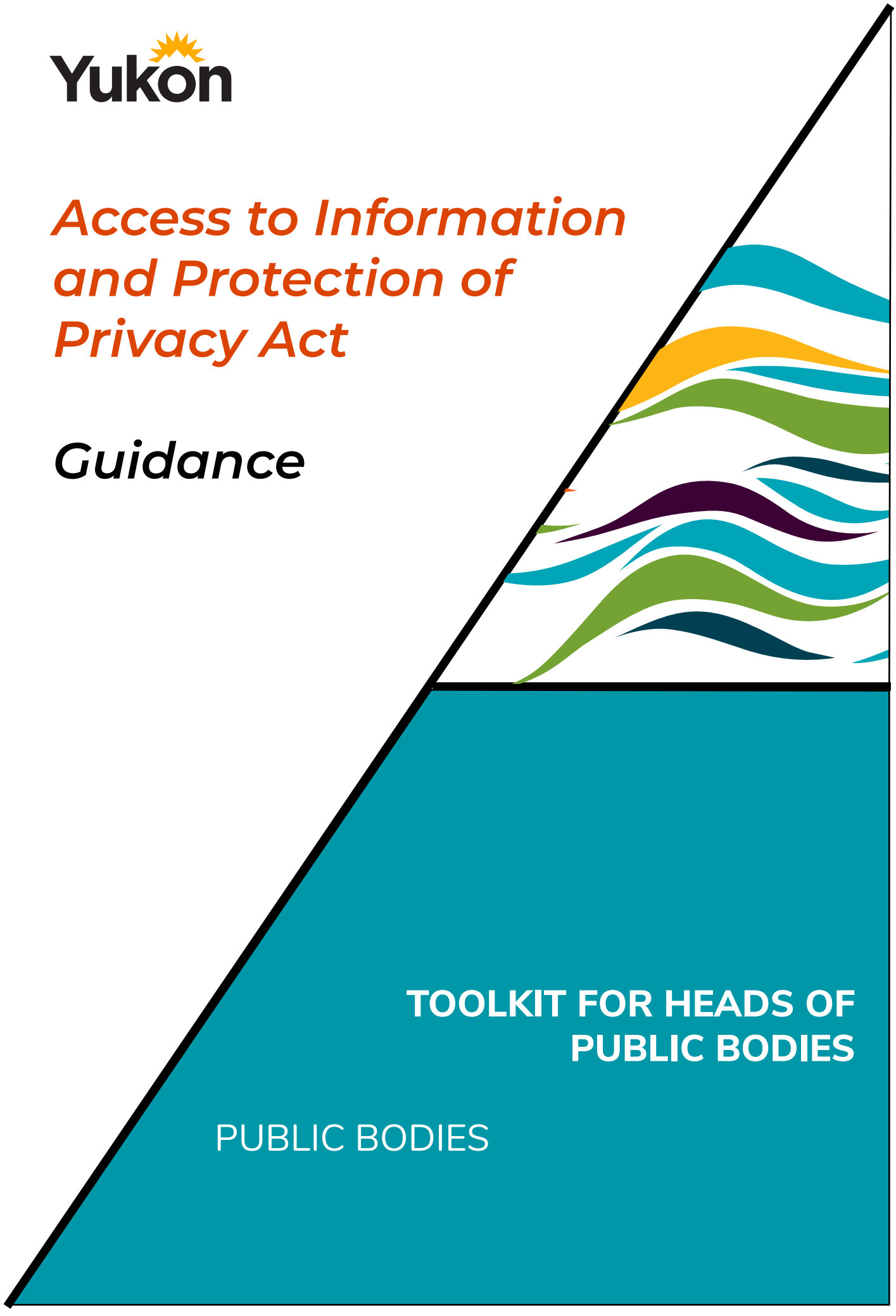
Yukon

Access to Information and Protection of Privacy Act

Guidance



TOOLKIT FOR HEADS OF PUBLIC BODIES

PUBLIC BODIES

TABLE OF CONTENTS

PURPOSE

The purpose of this toolkit is to help the Heads of Ministerial public bodies under-stand their powers and duties under the *Access to Information and Protection of Privacy Act (ATIPP Act)*.

The toolkit provides instruction on:

- The new roles created in the Act;
- The core responsibilities of each roles;
- Appointing the designated officers;
- Newly legislated activities, including recommendations to assist Heads for com-pliance.

To complement this toolkit, the ATIPP Office has created online training for Heads, as well as templates to assist with delegations and appointing Designated Access Officers and a Designated Privacy Officer.

The online training will be made available through YGLearn.

ROLES AND RESPONSIBILITIES IN THE *ATIPP ACT*

The *Access to Information and Protection of Privacy Act*, commonly referred to as the *ATIPP Act*, establishes the following roles and responsibilities. For the purposes of the *ATIPP Act*, public bodies include the Head, employees and service providers.

1 Head

The *ATIPP Act* definition of **"HEAD"** of a Ministerial public body is the MINISTER.

For the purposes of ATIPP, Ministerial public bodies have typically informally delegated their responsibilties to the Deputy Minister. Under the new *ATIPP Act*, this delegation will be formalized through a delegation document (see more information under section 6 of this document).

This clearly defined role of the Head in the Act has been made to increase accountability and expand the scope of the Act. Information and records held by the Head and their office will now be subject to the new Act.

The Head (or delegate) is responsible for decisions made under the Act that relate to their public body. These responsibilities include:

- Appointing designated officers for the public body;
- Receiving reports of employees not providing records to the Designated Access Officer within requested timelines;
- Conducting privacy impact assessments;
- Responding to requests for information from the Designated Privacy Officer related to suspected unauthorized collection, use or disclosure of personal information;
- Making decisions regardign the lack of notification for collection of personal information;
- Disclosing personal information related to threats to public health or safety, or for evaluating the performance of an employee;
- Securing personal information against a privacy breach;
- Receiving recommendations from the Information and Privacy Commissioner on breach reports and determining whether to apply actions based on the recommendations;
- Personal information corrections requests;
- Publishing public body information in the Open Access Register;
- Final decision on access requests including responses and consultations. Must submit time extensions in conjunction with recommendations from the Designated Access Officer to either the Access and Privacy Officer or Information and Privacy Commissioner
- Responding to a compliance inspection by the Access and Privacy Officer or an investigation by the Information and Privacy Commissioner.

The Head works closely with their Designated Access Officer(s) to receive recommendations, review and request revisions of the final response. Employees of public bodies support the Head, to ensure information *is* provided and the *ATIPP Act* is respected.

If an employee does not respond to their Designated Access Officer, the Act required the DAO to report the name and position of the individual to the Head. The title of a non-responsive employee is required in the Access Information Summary, which is provided to the Access and Privacy Officer. This may result in a compliance inspection audit by the ATIPP Office.

The Head also receives recommendations from the Access and Privacy Officer and the Information and Privacy Commissioner.

2 Access and Privacy Officer

The **"ACCESS AND PRIVACY OFFICER" (APO)** is an employee appointed by the Minister responsible for the Act (Minister of Highways and Public Works).

The APO provides oversight and advice to the Heads, Designated Access Officers and Designated Privacy Officers. This responsibility is intended to allow government to proactively assess and measure compliance.

The APO is responsible for accepting and refusing access requests, estimating costs, waivers for fees, extensions, compliance audits on public bodies, establishing an Access to Information Registry and publishing information related to compliance, including protocols. This helps to ensure that public bodies are following the rules on standardardization and compliance under the Act.

Other responsibilities include:

- Implementing policies, guidelines and procedures related to the management of a public body's compliance with the ATIPP Act;
- Ensuring the public bodies understand their roles under the Act;
- Providing advisory services to employees of Ministerial public bodies;
- Providing training on access and privacy to Ministerial public bodies;
- Providing information to the public on how the ATIPP Office operates and information on the Act;
- Managing the ATIPP Shared Services, which may include:
  - Monitoring and tracking the processing of requests;
  - Meeting legislated timelines and notification requirements
- Reviewing third party concerns related to access; and
- Calculating fee estimates.

3 Designated Access Officer

The Head of a Ministerial public body is required to designate one or more employees of a public body as their **"DESIGNATED ACCESS OFFICER" (DAO)**. This role replaces the role of ATIPP Coordinators and allows for flexibility of future decision-making. It permits the Head to appoint an employee from the public body (decentralized model) or appoint an employee from another public body (shared services model) as the Designated Access Officer.

DAOs report directly to the Head (or designate) of the public body. They are responsible for discharging the public body's statutory duties of processing access requests under Part 3 (Access to Information).

Other responsibilities include:

- Requesting relevant information from employees of the public body in order to respond to an access request;
- Notifying the Head of lack of response by an employee;
- Completing an Access Information Summary;
- Analyzing and severing information to which mandatory and/or discretionary exceptions to access apply;
- Making recommendations on access responses to the Head; and
- Receiving direction from the Head of the public body.

ATIPP Office Shared Services

Ministerial public bodies who opt into the ATIPP Office's Shared Services will designate a position within Shared Services as their Designated Access Officer. One or more employees may be designated as an access officer for several public bodies, to facilitate the shared service. The ATIPP Office will be responsible for assigning ATIPP files among a pool of analysts. As a Designated Access Officer, an assigned analyst will provide their recommendations to the Head of the public body. The Head will make the final decision on release.

The ATIPP Shared Service will help Ministerial public bodies provide subject-matter expertise in responding to access requests and assist Designated Privacy Officers with privacy breach assessment and responses.

Decentralized Ministerial Public Bodies

Ministerial public bodies that do not enter into a service level agreement with the ATIPP Office's Shared Services will be required to designate one or more employees of the public body as a Designated Access Officer. The public body is responsible for ensuring access and compliance under the Act including following protocols issued by the ATIPP Office, but will not receive the same level of support as the ATIPP Shared Services model on access requests.

4 Designated Privacy Officer

Each public body is required to designate one employee as the **"DESIGNATED PRIVACY OFFICER" (DPO)** to ensure that public accountability is maintained when dealing with privacy matters. The DPO reports directly to the Head (or designate) of the public body.

The name of the DPO should be circulated within the organization and staff should be encouraged to discuss privacy issues. The title and contact information of each DPO will also be made available to the public.

A public body may designate one employee to serve as both their Designated Access Officer and Designated Privacy Officer. This model will serve mostly smaller public bodies that do not have the capacity to facilitate separation between the roles. If a public body chooses to appoint an employee of another public body as their Designated Privacy Officer, the Heads of both public bodies should contact the ATIPP Office for assistance with outlining the services using a template provided by the ATIPP Office.

It is strongly recommended for large public bodies that collects and hold a significant amount of personal information to appoint an employee of their own public body to carry out the privacy responsibilities.

The Designated Privacy Officer is responsible for:

- Receiving reports of suspected unauthorized collection;
- Receiving reports of suspected privacy breaches (unauthorized use and disclosure);
- Assessing and responding to a privacy breach.

5 Information and Privacy Commissioner

The **"COMMISSIONER"** or Information and Privacy Commissioner (IPC) is a statutory officer created under the *ATIPP* Act. The Act also establishes the Office of the Information and Privacy Commissioner (OIPC).

The Commissioner is appointed by the Legislated Assembly and performs their statutory (legal) duties under the *Access to Information and Protection of Privacy Act*, as an Officer of the Legislative Assembly.

The Commissioner may receive and review complaints related to:

- Personal information corrections;
- Privacy complaints submitted by an individual or third party;
- Fee estimates;
- Waiver refusals;
- Refusals of access; and
- Abandonment of requests.

6 Delegation and Designation Process

Delegation of Duties and Powers

In accordance with the *ATIPP Act*, Heads of public bodies must formally delegate their *ATIPP Act* responsibilities using the Delegation Template provided by the ATIPP Office.

The Act expressly states Heads cannot delegate their power to a delegate. Once duties and powers are delegated by the Minister, Deputy Ministers or Designated Officers cannot re-delegate their responsibilities to another employee.

Any change in a previously delegated position requires the Head (Minister) to complete a new delegation form.

Signed delegation forms must be provided to the ATIPP Office and will be made public through the Access to Information Registry.

Designating Officers

Heads of Ministerial public bodies must formally designate the following statutory positions:

- Designated Access Officer (DAO)
- Designated Privacy Officer (DPO)

Any change in a previously delegated position requires the Head (Minister or delegate) to complete a new delegation form.

Heads may choose to delegate more than one employee as a Designated Access Officer, to ensure the public body has a standing alternate available.

As a reminder, only one Designated Privacy Officer may be appointed for each public body.

Signed delegation forms must be provided to the ATIPP Office and will be made public through the Access to Information Registry.

See Delegation and Designation Form Templates provided at the end of this toolkit.

7 Recommended Core Competancies

Designated Access Officer

A Designated Access Officer is a highly technical, analytical position that involves attention to detail and the ability to interpret and apply law to records held by a public body.

These five core competancies represent the basic expectations and achievements fo an individual who will be sucessful in the role.

It is important to choose one or more individuals who have experience interpreting legislation researching policies and case law to effectively meet the requirements of this role under the *ATIPP Act*.

EDUCATED	• Public Administration, Information Management, Law or Paralegal Studies
EXPERIENCED IN LAW	• Can interpret and apply law to information • Experienced in access legislation and privacy legislation
RESEARCH AND ANALYSIS FOCUSED	• Researching, interpreting and analyzing legislation, policies and case law
CLIENT FOCUSED	• Client service orientated with excellent written and oral communication skills
INTERPERSONAL & COMMUNICATION SKILLS	• Prioritizes work and manages deadlines, able to work independently and collaboratively

Designated Privacy Officer

A Designated Privacy Officer is a confidential, investigatory position that involves tact, empathy, discretion and an in-depth understanding of privacy, information management and information technology.

It is important to choose an individual who has the skill set required to build capacity and relationships within their public body and to be viewed as a trusted individual.

Assessing and responding to a report of a suspected privacy breach, or auditing a program or activity's collection practices requires a strong, knowledgeable individual who can communicate the *ATIPP Act*'s legal requirements to program staff.

Building a rapport is essential to the fact-finding and evaluation skills required for a successful breach evaluation. Public body employees should understand the importance of the investigation, their legal responsibilities and why their cooperation is required to complete the investigation.

These five core competancies represent the recommended knowledge and skills to ensure Designated Privacy Officers can succeed in fulfilling the role's responsibilities.

EDUCATED	• Privacy law, Information Management, Cyber Security, Public Administration
PRIVACY FOCUSED	• Experience interpreting privacy legislation • Knowledge of Canadian Standard Association's Ten Privacy Principals
KNOWLEDGEABLE IN INFORMATION MANAGEMENT & IT	• Knowledge and understanding of Information Management Principals (physical and electronic records) • Basic knowledge of Information Technology (IT) Security • Business process mapping
INVESTIGATION SKILLS	• Ability to assess breaches, conduct investigations and gather evidence to make findings and recommendations
INTERPERSONAL & COMMUNICATION SKILLS	• Ability to maintain relationships in a confidential setting, utilize diplomacy, empathy and tact while dealing with sensitive, confidential matters

8 Recommendations for Compliance

Heads are required to comply with all responsibilities as outlined in the ATIPP Act. This includes making all public body employees (including service providers) aware of their statutory requirements within the *ATIPP Act*, *ATIPP Act Regulations* and the *ATIPP Act Protocols*.

Failure of the Head or any public body employee to comply with the *ATIPP Act*, *Regulations* or protocols may result in:

- A compliance inspection audit by the ATIPP Office, or
- an investigation by the Office of the Information and Privacy Commissioner (OIPC).

Among the most significant changes in the Act for Heads, are the Open Access Division and Privacy Impact Assessments. In order to meet these new statutory requirements, Heads may wish to implement the following recommendations for compliance. These recommendations will help Heads identify which roles or positions are available to carry out these new requirements.

Open Access Publishing Requirements (Part 3, Division 2)

POLICY AND COMMUNICATIONS BRANCH

It is recommended that communications staff, currently responsible for publishing on Yukon's Open Data site and Yukon.ca, have the responsibility to perform duties under the Open Access Division. Therefore, it is recommended that they be assigned the Open Access requirements that will be provided by the Departments of Highways and Public Works, eServices unit.

PROJECT MANAGERS/PROGRAM STAFF

Privacy Impact Assessments (PIAs) are now a requirements under the *ATIPP Act*. It is recommended that project managers and program staff, with the assistance of the ATIPP Office, lead these privacy impact assessments. Staff participation in PIAs ensures they have the subject matter expertise that is critical to completing these PIAs and gaining approvals. It also ensures that they are compliant with the *ATIPP Act Protocols*.

Depending on the type of PIA required, a PIA may take 1-2 days (low complexity), 2 weeks (medium complexity) or 1 month or longer (high complexity) to complete.

Highly complex PIAs may require a PIA Development Team on the advice from the ATIPP Office. This team may include business analysts, project managers, Information Management (IM) employees, Information Technology (IT) employees, ICT support (HPW), Security Officers (HPW), Privacy Compliance Specialists (ATIPP Office) and outside contractors supplied through the ATIPP Office.

The ATIPP Office has established Qualified Source Lists for Privacy Impact Assessments (PIAs) and Security Threat Risk Assessments (STRAs) with instructions for secondary procurement to ensure documents meet the requirements of the ATIPP Office and Chief Information Secuirty Officer (CISO).

DELEGATION BY THE HEAD OF THE PUBLIC BODY

Name of public body	

Pursuant to section 88(c) of the *Access to Information and Protection of Privacy Act*, I hereby delegate my powers, duties and functions as Head of the public body to the Deputy Minister.

For the purposes of the functions listed below, I hereby delegate the functions listed as Head of the public body to the Designated Access Officer:

(a) requests for extensions to the Access and Privacy Officer and the Information and Privacy Commissioner;

(b) seeking a third party's view on granting access; and

(c) consulting with the Access and Privacy Officer before the Access and Privacy Officer decides whether to accept or refuse an access request.

For the purposes of the functions listed below, I hereby delegate the functions listed as Head of the public body to the director responsible of the program or activity of the public body:

(a) conducting Privacy Impact Assessments; and

(b) providing notice to the Commissioner whether recommendations will be accepted or rejected.

The above delegations are subject to the following conditions:

(a) that the persons to whom my powers, duties or functions are delegated are bound in the exercise of those powers, duties or functions by the legislative and

administrative limitations to which I am subject;

(b) that the powers, duties or functions delegated to any person may also be exercised by another person who holds the person's position in an acting capacity to which he or she has been duly appointed;

(c) that delegation does not limit the authority of individuals in positions directly above the listed positions to exercise any of the delegated powers, duties, or functions in their area of responsibility; and

(d) that notwithstanding the delegation of my powers, duties or functions, I may exercise at any time any of the powers, duties or functions delegated.

This delegation is effective on and from the date shown below and shall remain in effect until revoked. This delegation may be revoked or amended from time to time.

Deputy Minister	Signature	Date

Minister	Signature	Date

CC: ATIPP OFFICE

DESIGNATION OF ACCESS OFFICER BY THE HEAD OF THE PUBLIC BODY

Name of public body	

Pursuant to section 87(1)(a) of the *Access to Information and Protection of Privacy Act*, I hereby designate the following position(s) as the **Designated Access Officer** of the public body, subject to the following conditions:

(a) that the persons designated with powers, duties or functions as this statutory officer are bound in the exercise of those powers, duties or functions by the legislative and administrative limitations to which they are subject;

(b) that the powers, duties or functions designated to this position may also be exercised by any person in an acting capacity to which he or she has been duly appointed;

This designation is effective on and from the date shown below and shall remain in effect until revoked. This delegation may be revoked or amended from time to time.

Deputy Minister	Signature	Date

CC: ATIPP OFFICE

DESIGNATION OF PRIVACY OFFICER BY THE HEAD OF THE PUBLIC BODY

Name of public body	

Pursuant to section 87(1)(a) of the *Access to Information and Protection of Privacy Act*, I hereby designate the following position as the **Designated Privacy Officer** of the public body, subject to the following conditions:

(a) that the persons designated with powers, duties or functions as this statutory officer are bound in the exercise of those powers, duties or functions by the legislative and administrative limitations to which they are subject;

(b) that the powers, duties or functions designated to this position may also be exercised by any person in an acting capacity to which he or she has been duly appointed;

This designation is effective on and from the date shown below and shall remain in effect until revoked. This delegation may be revoked or amended from time to time.

Deputy Minister	Signature	Date

CC: ATIPP OFFICE