OLG CORPORATE POLICY

TITLE: **Freedom of Information & Privacy Legislation**

POLICY # : **CP-01-01-001**

OWNER: **Legal – Information Access and Privacy**

STATUS: **Final**

Table of Contents

PURPOSE

The purpose of this policy is to:

- Set out the governing process for establishing and maintaining a Freedom of Information (FOI) and privacy program at Ontario Lottery and Gaming Corporation (OLG) in accordance with the *Freedom of Information and Protection of Privacy Act* (FIPPA) RSO 1990 and Regulations
- Establish an organizational culture that is aware of our obligations to make information accessible to the public and protect personal and other information
- Promote OLG compliance with FIPPA

APPLICATION AND SCOPE

This policy applies to all OLG staff. Contract workers, temporary employees, and external vendors and service providers are also bound by contractual provisions to meet FOI and privacy requirements.

This policy applies to all information in the custody or control of OLG irrespective of its format, storage or medium. It does not apply to information that is excluded under section 65 of FIPPA.

POLICY STATEMENT

The purposes of FIPPA are:

a) to provide a right of access to information under the control of Ontario Government institutions
b) to protect the privacy of individuals with respect to personal information about themselves held by Ontario Government institutions and to provide individuals with a right of access to that information

OLG supports the principles of FIPPA as well as the concept of Privacy by Design promoted by the Ontario Information and Privacy Commissioner, and will make every effort to embed privacy into the design and architecture of business systems and processes.

DEFINITIONS

President/Chief Executive Officer (CEO): OLG's P/CEO who is the official designated as the head for making decisions under FIPPA.

Coordinator/Manager: the person designated by OLG to manage FOI and privacy programs.

Delegate: the official to whom the head's powers and duties, as set out in FIPPA, have been delegated.

Delegation of Authority (DOA): is a written document setting out the duties and/or functions that have been assigned to official(s) in the institution other than the head to carry out.

Directory of Records: a publication required by FIPPA that describes the type of records and manuals maintained by Ontario government institutions, including personal information banks.

Head: the official designated under FIPPA responsible for making decisions with respect to access to information (FOI requests), protection of records, and for ensuring that personal information is managed in accordance with privacy requirements.

Information and Privacy Commission of Ontario (IPC): the Ontario government organization that acts independently to uphold and promote open government and the protection of personal privacy.

Institution: an organization subject to FIPPA and includes OLG.

Personal information: information about an identifiable individual as defined by section 2(1) of FIPPA.

Personal Information Bank: a collection of personal information that is organized and capable of being retrieved using an individual's name or an identifying number or particular assigned to the individual.

Privacy Breach Guidelines: a set of guidelines posted on InsideOLG to guide OLG employees in the identification and handling of potential privacy breaches.

Privacy Impact Assessment (PIA): a process/tool that helps to determine whether new technologies, information systems, initiatives and/or proposed programs or policies meet privacy requirements.

Record: any record of information however recorded, whether in printed form, on film, by electronic means or otherwise.

FOI Request: a written request from a person seeking access to a record under FIPPA.

REQUIREMENTS

1. Compliance with FIPPA

1.1. OLG will designate a Coordinator/Manager to manage the FOI and privacy programs as well as additional staff as required to execute the programs.

1.2. Appropriate protocols, tools and training modules on the requirements of FIPPA will be available to staff.

2. Collection, use and disclosure of personal information

2.1. Personal information will be collected, used and/or disclosed in accordance with FIPPA.

2.2. Whenever personal information is collected, used and/or disclosed, a Notice of Collection will be provided which details OLG's authority to collect personal information, specifies the intended use(s) of the personal information and provides contact information for questions about the collection. Where applicable, appropriate consent will also need to be acquired.

2.3. OLG will safeguard personal information that it collects, uses and/or discloses through security protocols and policies (see Related Policies and Procedures section) and education of staff on the handling of personal information.

2.4. Privacy considerations will be embedded in the systems, design, and architecture of OLG's programs and processes whenever personal information is collected, used and/or disclosed.

3. Access to personal information

3.1. Access to personal information will be restricted to authorized personnel who need it to carry out their responsibilities.

3.2. Individuals may request access to records containing their personal information in accordance with FIPPA and OLG's privacy policies.

4. Retention and disposal of records (including those that contain personal information)

4.1. Records will be retained in accordance with FIPPA and other relevant legislation and directives, as well as related OLG policies (see Related Policies and Procedures section).

4.2. Records that are slated for disposal will be destroyed securely in accordance with OLG retention schedules and relevant policies (see Related Policies and Procedures).

5. Posting of Public Policy

5.1. OLG will post a privacy statement on its public website providing details about the collection, use and/or disclosure, as well as the security of personal information gathered by OLG, including information gathered via OLG's websites.

ROLES AND RESPONSIBILITIES

The P/CEO as 'head of the institution' is responsible for:

- Overseeing compliance with applicable FIPPA policies, directives, Memorandums of Understanding (MOUs) and guidelines
- Designating a Coordinator/Manager for access and privacy matters
- Ensuring that structures and procedures have been established for implementing and complying with FIPPA
- Signing a delegation of authority (DOA) document if the head's powers and duties are to be delegated (see Appendix A)

Executive Leadership Team members are responsible for:

- Carrying out any powers or functions delegated by the P/CEO in a DOA
- Establishing appropriate processes and resources, including divisional representatives, to respond to FIPPA requests within legislated timeframes
- Incorporating privacy considerations into systems, processes, policies and procedures where possible
- Consulting with Information Access and Privacy Services regarding any initiative involving personal information to determine whether a Privacy Impact Assessment (See Appendix B) is required
- Providing appropriate resources, as required, to work with Information Access and Privacy Services in the handling of privacy breaches/complaints

FIPPA Coordinator/Manager is responsible for:

- Planning and managing OLG's FIPPA and privacy programs, including facilitating timely responses to FOI requests
- Providing advice to senior management on access and privacy issues
- Liaising with the Information and Privacy Commission, legal counsel and others as required on FOI and privacy related matters
- Investigating and reporting on privacy breaches and/or complaints
- Managing and making available to staff, tools and training modules with respect to FOI and privacy.

Information Access and Privacy Services staff are responsible for:

- Responding to FOI Requests and ensuring compliance with FIPPA requirements and legislated timeframes for responding to FOI requests.
- Providing advice and assistance to OLG staff on FOI and privacy matters
- Responding to requests for the correction of personal information
- Managing and updating OLG's entry in the Directory of Records in compliance with FIPPA requirements
- Preparing and submitting an annual statistical report to the IPC regarding response rates with respect to legislated timeframes for responding to FOI requests
- Supporting the Coordinator/Manager in liaising with the IPC during the appeals process for FOI requests, investigating privacy breaches and/or complaints, and providing training on FOI and privacy
- Conducting Privacy Impact Assessments

Divisional FIPPA Representatives are responsible for:

- Establishing procedures to ensure the retrieval of records is complete, accurate and timely in response to FOI requests
- Identifying and retrieving records in response to FOI requests
- Identifying issues that may have an impact on the release or denial of access to records

Document Management Services staff are responsible for:

- Managing physical records of OLG
- Destroying physical records that have expired their time period in accordance with Document Management Services' record retention schedules.

Information Security Office staff are responsible for:

- Establishing enterprise security programs for protecting personal information

OLG Employees are responsible for:

- Participating in FIPPA training as required and adhering to the requirements of this policy and other OLG policies (see Related Policies and Procedures section) related to management of personal information

POLICY OWNER

Legal – Information Access and Privacy

RELATED POLICIES AND PROCEDURES

- CP-02-07-003: Records Management – Off-Site Storage Services
- FP-04-08-002: Mobile Communication Devices
- FP-04-05-009: Information Classification and Handling
- FP-04-05-013: Application Service Provider Security
- CP-04-05-018: Third Party Access
- FP-04-05-019: Data Protection
- OLG Information Classification and Handling Procedures

REFERENCES AND FORMS

- *Freedom of Information and Protection of Privacy Act* (FIPPA) RSO 1990, and Regulations
- Ontario Public Service Freedom of Information Guideline
- Ontario Public Service Privacy Impact Assessment Guidelines
- Introduction to Privacy by Design (PbD) http://www.ipc.on.ca/english/Privacy/Introduction-to-PbD/

REVISION / REVIEW HISTORY			
Version/Revision Date	**Requested By**	**Updated By**	**Summary of Revision**
July 27, 2015	Senior Mgr. Information Access & Privacy	Policy Services	Updated roles section to reflect correct title of P/CEO and that IA&P staff provide assistance on privacy matters as well as FOI.
February 14, 2013	Senior Manager, Information Access & Privacy Services	Senior Manager, Information Access & Privacy Services	Revised and updated policy statement, definitions, requirements, and roles & responsibilities sections.

APPROVALS		
Approver	**Authorization**	**Date**
Bernard Woo Senior Mgr. Information Access & Privacy	Signature on file	July 29, 2015

EC / VP / BOARD OF DIRECTORS APPROVAL	
Approved By	**Authorization Date**
Original version approved by Executive Committee	April 19, 2010

APPENDIX A – DELEGATION OF AUTHORITY

A delegation of authority (DOA) occurs when one person, who is responsible and accountable for the duties of a function (that is either required by legislation or policy), assigns those duties to another person to execute. Individuals delegating duties to someone else remain accountable for actions taken and decisions made.

Delegation of the head's powers

Section 62(1) of the Act provides that a head "may in writing delegate a power or duty granted or vested in the head to an officer or officers of the institution or another institution subject to such limitations, restrictions, conditions and requirements as the head may set out in the delegation".

The head is not legally required to delegate his/her authority; however section 62(1) was introduced to recognize that while there needs to be an official with ultimate responsibility for the Act, the most senior official in an organization likely does not have the time to actively manage the Act's many legal and administrative obligations.

The DOA is a written document and Legal Counsel should draft the DOA to ensure it addresses all of the FIPPA legal obligations. Once completed and approved, the DOA should be circulated to all officials with delegated responsibilities and they should formally acknowledge having reviewed the delegation**.**

APPENDIX B – PRIVACY IMPACT ASSESSMENTS & CHECKLIST

What is a Privacy Impact Assessment (PIA)?

- A process/tool that helps to determine whether new technologies, information systems, proposed programs, policies or initiatives meet privacy requirements
- It measures compliance with the *Freedom of Information and Protection of Privacy Act* (FIPPA) R.S.O. 1990, c.F.31 and identifies the broader privacy implications of a given proposal
- Once completed, the PIA report will contain an analysis of the privacy issues raised by the proposal and recommendations for mitigating any risks that have been identified

What is the Goal of a Privacy Impact Assessment?

- Ensure that privacy is considered throughout the project development cycle including the design phase
- Generate and communicate confidence that privacy objectives have been met, and promote fully informed policy decision-making and system design choice
- Anticipate public reaction to the privacy implications of a given proposal, and eliminate the need for costly system re-engineering due to public criticism

What are the benefits of a Privacy Impact Assessment?

- Promotes awareness of privacy concerns
- Anticipates privacy issues and acts as an "early warning" management tool
- Provides senior management with options to avoid privacy risks

Introduction

As a government agency, OLG is subject to the *Freedom of Information and Protection of Privacy Act* (FIPPA) R.S.O. 1990, c.F.31. The legislation restricts how government organizations can collect, use and disclose personal information. The collection of personal information at OLG must be necessary and appropriate for carrying out a "lawfully authorized activity" (ie: carrying out our business) and may require the consent of the individual to whom the personal information relates.

The term "collection" means that personal information is actively sought, retained and used by OLG. When personal information is collected we must inform the individual of our authority to collect the information, what the information is being used for, and provide the name and number of someone who can answer any questions the individual may have regarding the collection of their information.

The collection of personal information must also be directly from the individual to whom the information relates and can only be used for the purpose it was collected. Personal information collected for one purpose cannot be used for any other purpose unless the individual consents.

The disclosure of personal information is also restricted to specified circumstances such as when the individual to whom the information relates consents to the disclosure or to comply with another piece of legislation. This restriction means that internally within OLG, the disclosure of personal information is restricted to employees who need the information to carry out their job.

Section 2 of FIPPA defines personal information as "recorded information about an identifiable individual". It includes both traditional paper records and electronic records (i.e. emails, texts, word files, spreadsheets, audio and video tapes). Examples of personal information may include an individual's:

- Address
- Telephone number
- Email address
- Date of birth
- Gender
- Marital/family status
- Education/medical /employment history
- Financial transactions
- Identifying number (e.g. driver's license number)

Note: the list above is <u>not</u> exhaustive and other information may be considered personal information.

The purpose of the Privacy Checklist is to assist OLG employees in assessing whether a given proposal, program or project ("initiative"), either new or currently operational, involves the collection, retention, use and/or disclosure of personal information and is being carried out in a manner consistent with the requirements of FIPPA. The questions in the Privacy Checklist will assist in determining whether a privacy analysis is required to ensure that privacy requirements are reasonably met.

The completed checklist should be forwarded to Information Access and Privacy Services (IAPS) along with all relevant and available documents. Documents that should be forwarded to IAPS are noted in the appropriate section of the checklist.

If you need assistance completing the checklist or have any questions, contact:

- Bernard Woo, Senior Mgr. Information Access & Privacy
  416-224-7080 ext. 6546, bwoo@olg.ca

Privacy Checklist			
Section 1: Background information			
a. Name of initiative:			
b. Provide a brief description of the initiative.			
c. Does the initiative have a "go live" date? If "Yes", what is it? (YY/MM/DD)			
Section 2: Key contacts/stakeholders			
Title/Role	Name	Business Phone Number	Business Email Address
a. Project Sponsor/Business Owner: (OLG employee with overall responsibility for the initiative)			
b. Business Lead: (OLG employee with day-to-day responsibilities for the initiative)			
c. Project Manager (if applicable):			
d. Other key contacts/stakeholders (if any, leave blank if none):			

Section 3: Personal Information	**Yes**	**No**
a. Will any personal information, as described in this checklist be collected, used and/or disclosed?		
b. Is the collection use or disclosure reasonably necessary and appropriate to the effective execution of the initiative?		
c. Describe the personal information being collected, used and/or disclosed.		

Section 4: Collection of Personal Information	Yes	No
a. Will the initiative involve a new collection of personal information? E.g. will it involve an individual providing their personal information to OLG?		
b. If the answer to a. is Yes, indicate how the information will be collected.		

Section 5: Use/ Disclosure of Personal Information	Yes	No
a. Will the initiative involve the use/disclosure of personal information?		
If the answer to a. is Yes, answer the following three questions:		
b. Was the personal information previously collected for another purpose? Describe the purpose of the previous collection.		
c. Has or will consent be obtained to use/disclose the personal information?		
d. How will the personal information be used/disclosed?		

Section 6: Information Technology (IT)	Yes	No
a. Will the initiative involve an IT system or solution?		
Note: Forward all requirements documents, such as the Business Requirements Document (BRD), Product Requirements Document (PRD), Non-Functional Requirements Document (NFR), to IAPS along with the completed checklist, even if the document is only in draft status.		

End of checklist