Legislative Policy 3.01

Subject: **PROTECTION OF PRIVACY AND CONFIDENTIALITY OF INFORMATION**

Scope: **WARDEN, MEMBERS OF COUNTY COUNCIL, MIDDLESEX COUNTY LIBRARY BOARD AND ALL EMPLOYEES OF MIDDLESEX COUNTY AND MIDDLESEX COUNTY LIBRARY**

Issued: **October 24, 2017**

Revised:

Purpose

The purpose of the Protection of Privacy and Confidentiality of Information policy is to;

- ensure the protection of personal information, personal health information and confidential information and how it is collected, retained, used, disclosed and disposed of by Middlesex County,
- provide a right of access to individuals with respect to personal information about themselves,
- ensure individuals have access to information which is not considered to be personal information, personal health information or confidential information,
- establish procedures to assure the public that Middlesex County takes privacy and confidentiality of information seriously by taking proactive measures during program development and service delivery,
- identify what Personal Information, Personal Health Information and Confidential Information is, and,
- establish investigation and reporting procedures for privacy breaches.

Definitions

For the purposes of this document, the following terms have the following meanings:

Confidential Information – is any and all information relating to the business, operations, personnel and affairs of the County and its assets which is not a matter of public record.

Departments – means any categorical division of service delivery or municipal administration of Middlesex County which is officially recognized by Middlesex County and exercises powers delegated to it by Middlesex County, including but not limited to any local board, as defined by the *Municipal Act*, 2001 as amended or replaced, which exercises powers delegated to it by Middlesex County.

Health Information Custodian ("Custodian") - is any person or organization involved in delivering health care services who has custody or control of the Personal Health Information of an individual.

Information Systems – is any hardware or software system that is used to collect, filter, process, create, store and distribute data.

Personal Health Information – is information whether oral or written which relates to the provision of health care to an individual.

Personal Information – is recorded information about an identifiable individual.

Personal Information Bank – is a collection of Personal Information that is organized and capable of being retrieved by an individual's name or other individual identifier.

Privacy Impact Assessment (PIA) – is a process for identifying, assessing and mitigating privacy risks. A PIA is a due diligence exercise to analyze the effects of a technology, system, program or service design on the privacy of individuals.

Record – is any form of information however recorded, whether in printed form, on film, by electronic means or otherwise held by the County.

Policy

In accordance with Middlesex County's policies, the Municipal Act, the Municipal Freedom of Information and Protection of Privacy Act ("MFIPPA") and the Personal Health Information Protection Act ("PHIPA"); Middlesex County ("the County") will protect the privacy and confidentiality of Personal Information, Personal Health Information and Confidential Information by ensuring appropriate procedures are in place to collect, retain, use, disclose and dispose of such information.

Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)

The purpose of MFIPPA as it relates to this policy is to;

1. Protect individual privacy by:
    - Requiring the County to handle Personal Information in accordance with the collection, use, retention, disclosure and disposal rules under MFIPPA.
    - Providing the right to Ontarians to complain to the Information and Privacy Commissioner (IPC) if they feel the County has mishandled their Personal Information.
2. Ensure all persons have a right of access to their Personal Information and can request its correction.

Personal Information

Personal Information shall not be disclosed to anyone except those authorized to use it for purposes which are consistent with the original reason it was collected for.

Personal Information can include, but is not limited to:

- an individual's biographical details (name, sex, age, race),
- an individual's biological details (face, fingerprints, blood type, etc.),
- nationality,
- religion,

- marital status,
- education,
- medical or criminal history,
- financial information,
- identifying numbers, for example, Social Insurance Numbers,
- an individual's contact details (personal address, phone number, etc.) and
- personal opinions and views.

1. All employees, volunteers and members of Council have the responsibility to protect the Personal Information they collect, retain, use, disclose and dispose of during County business. Personal Information must be secured and protected from unauthorized access at all times.
2. Personal Information must only be used for purposes which are consistent with the original reason it was collected for.
3. Notice of Collection, Privacy Statements and Contact Information shall be communicated to the Public when Personal Information is being collected.
4. Privacy training is mandatory for all employees, volunteers and members of Council who may handle Personal Information.
5. Personal Information shall only be accessed by authorized individuals for the purpose of performing their regular duties.
6. Personal Information shall not be removed from County premises or Information Systems unless the appropriate authorization is provided.
7. If Personal Information must be transported, every effort must be taken to ensure it is secure and protected from unauthorized access or distribution. Refer to Appendix "A" for more details.
8. Personal Information must be treated as Confidential Information.

Confidential Information

Confidential Information shall not be disclosed to anyone except those who are authorized and who require the information for legitimate business purposes.

Confidentiality is demonstrated in the following ways:

- an explicit statement of confidentiality,
- a written or verbal request for confidentiality,
- the County's treatment of the information as sensitive or confidential.

Confidential Information however identified is only as confidential as how it is treated. Confidential Information must actually be treated as confidential.

Confidential Information recorded on paper, for example, must be:

- stored in secure cabinets (locked when not in use, not in a public space, with access only to authorized persons),
- secured within a file folder / cover paper when outside of the secure cabinet,
- returned to the secure cabinet when not in use, and
- accessed only by authorized staff on a "need to know" basis.

Confidential Information recorded in electronic form, for example, must be:

- protected using passwords and other appropriate methods to restrict access to computers and computer networks,
- protected by encrypted storage media when files are in transit, and
- accessed only by authorized persons on a "need to know" basis.

Confidential Information shall not be removed from County premises or Information Systems unless appropriate authorization is provided.

Personal Health Information

Personal Health Information Protection Act ("PHIPA")

The Personal Health Information Protection Act sets out rules for the collection, use and disclosure of Personal Health Information. Personal Health Information is considered as one of the most sensitive forms of information that must be protected from unauthorized or unintentional collection, use or disclosure.

Departments considered to be Health Information Custodians or Departments which provide services to Health Information Custodians must ensure the appropriate policies and procedures are in place that adhere to the rules for the collection, use and disclosure of Personal Health Information as outlined in Ontario's Personal Health Information Protection Act.

Some examples of Health Information Custodians ("Custodians") are health care practitioners, long-term-care service providers, the Ministry of Health and Long-Term Care or Land Ambulance Services.

Additionally, the Personal Health Information Protection Act provides individuals the right to access and request correction of their own Personal Health Information.

Protecting Personal Health Information

Custodians must implement and follow information practices which comply with PHIPA and its regulations. These information practices must describe when, how and the purposes for which the Custodian routinely collects, uses, modifies, discloses, retains or disposes Personal Health Information including the administrative, technical and physical safeguards and practices that the Custodian has in place.

Custodians must make every reasonable effort to ensure Personal Health Information in their custody and control is protected from theft, loss and unauthorized use or disclosure. In the event Personal Health Information is stolen, lost or accessed by an unauthorized person, the Custodian must notify the affected individuals.

Collection, Use and Disclosure of Personal Health Information

PHIPA sets out general principles which apply to the collection, use and disclosure of Personal Health Information.

- A Custodian may only collect, use or disclose Personal Health Information if the individual consents or the collection, use or disclosure is permitted or required under the act;
- a Custodian must not collect, use or disclose Personal Health Information if other information will serve the purpose;
- a Custodian must not collect, use or disclose more Personal Health Information than is necessary to meet the purpose;
- express consent is required to collect, use or disclose Personal Health Information for marketing purposes;
- and any persons who are not Custodians or aren't authorized by a Custodian to act on their behalf must not collect, use or disclose Personal Health Information.

Access to Personal Health Information Records

With some exceptions, individuals have the right of access to records containing their own Personal Health Information. The right of access applies to a record that is dedicated primarily to the individual. However, if the record is not primarily about the individual, the right of access only extends to the portion which is about the individual.

Custodians must provide individuals access to their own Personal Health Information records unless;

- a legal privilege restricting disclosure applies;
- another law prohibits disclosure;
- the information was collected or created for a proceeding;
- the information was collected or created during an inspection, investigation or similar procedure;
- access could result in serious harm to any person or the identification of a person who was required to provide information or who was provided the information in confidence; or
- the Custodian is a government institution and the disclosure may be refused under certain provisions contained in access and privacy legislation that applies to government organizations.

If one of these exceptions apply, the Custodian should sever the record and provide access to the part of the record in which the exception does not apply.

All reasonable efforts should be made to ensure requests for access are in writing and provide enough information to allow the Custodian to identify and locate the record. In the interest of transparency, if the individual has not provided enough detail, under the act the Custodian is required to offer assistance.

If an oral request for access to an individual's Personal Health Information is received, the request must be appropriately recorded.

Correction of Personal Health Information Records

If an individual believes that a record of their Personal Health Information is not as accurate or complete as necessary for its purpose, the individual can make a written request to the Custodian to correct the record. The Custodian is required to correct a record that is not accurate or complete unless the Custodian did not create the record or the record consists of a professional opinion that was made in good faith.

If the incorrect information was disclosed to anyone, the individual may require the Custodian within reason to inform anyone of the incorrect information.

Complaints, Breaches and Reporting Requirements

All complaints and/or suspected breaches relating to the inappropriate, inadvertent or unauthorized collection, retention, use, disclosure or disposal of information in ways that are not consistent with MFIPPA, PHIPA or related County policies must be immediately contained, within reason and reported to the designated Privacy Officer.

a. Departments must have the proper reporting procedures in place which ensure barriers to efficient and effective reporting are minimized.

b. The loss or theft of Personal Information, Personal Health Information or Confidential Information must be immediately reported to the designated Privacy Officer so that appropriate action can be taken. For example, if Personal Information, Personal Health Information or Confidential Information has been lost through theft, the police will be notified.

c. If someone believes to have inadvertently disclosed Personal Information, Personal Health Information or Confidential Information, or is unsure if they have done so, the incident must be reported immediately to the designated Privacy Officer.

d. The Privacy Officer or delegate shall report the loss or theft of Personal Information or Personal Health Information to the Information and Privacy Commissioner of Ontario.

Location	Designated Privacy Officers
Strathmere Lodge Long-Term Care Home	Strathmere Lodge Administrator
All Other Middlesex County Departments	Middlesex County Clerk's Office

Privacy Impact Assessment (PIA)

1. Department Heads must ensure that a Privacy Impact Assessment ("PIA") is completed prior to implementing a new program or significantly changing an existing program that requires the collection, use or disclosure of Personal Information or Personal Health Information.
2. When a PIA is required, it is the responsibility of the Department Head or delegate to complete the PIA form and provide a copy to the County Clerk, Director of ITS and Director of Legal Services for review and feedback.
3. Completed PIA forms must be referred to throughout the project lifecycle to ensure that the protection of Personal Information is maintained.

Personal Information Banks

A Personal Information Bank is a collection of personal information that is organized and capable of being retrieved using an individual's name or an identifying number or another identifier assigned to the individual. For example, Payroll Database, Accounts Receivable, Library Patron Databases.

1. It is the responsibility of the Department Head in the custody and control of the Personal Information Bank to complete a Personal Information Bank Index Form (Appendix C) and submit it to the County Clerk.
2. Any changes relating to the Personal Information Bank must be provided to the County Clerk to ensure accuracy is maintained.

The County Clerk will ensure the Personal Information Bank is indexed, up to date and available on the Middlesex County website.

Department Policies and Procedures

Departments which collect, retain, use, disclose and dispose of Personal Information, Personal Health Information, Confidential Information or any other information which is protected by privacy legislation, must ensure that the appropriate departmental policies and procedures are in place, including but not limited to the;

- access of Personal Information, Personal Health Information or Confidential Information,
- the transportation of Personal Information, Personal Health Information or Confidential Information,
- protecting the privacy of Personal Information, Personal Health Information or Confidential Information when working outside of their primary office (refer to Appendix A), and,
- that employees understand that although they may be authorized to access specific Records within a set of information, they are not entitled to access all information which may be related.

Disposal of Personal Information, Personal Health Information or Confidential Information

There are a number of commonly accepted ways for departments to properly dispose of Personal Information, Personal Health Information or Confidential Information depending on the form in which it is being stored. The objective is to permanently destroy the media which stores Personal Information, Personal Health Information or Confidential Information so that it cannot be reconstructed or recovered in any way. When going through the process of disposal, a department should also destroy all associated copies and backup files.

Information is commonly stored on two types of media, hard (paper) copy or electronic copy.

Personal Information, Personal Health Information or Confidential Information which is stored on hard (paper) copy must be destroyed using a paper shredder or placed in a confidential document destruction bin.

Personal Information, Personal Health Information or Confidential Information which is stored on electronic storage media (electronic copy) must be destroyed using approved destruction methods as defined by the Information Technology Services (ITS) department. Please contact the ITS department to obtain an up to date document which outlines the secure and proper destruction methods of electronic storage media. Electronic storage media may also be submitted to the ITS department for the secure and proper destruction of electronic records.

Non-Compliance

Any persons found to be in violation of this policy may be subject to disciplinary action up to and including termination of employment.

APPENDIX A

IPC of Ontario – Guidelines for Protecting the Privacy and Confidentiality of Personal Information When Working Outside the Office

APPENDIX B

Personal Information Assessment Form

APPENDIX C

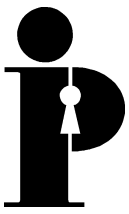
Personal Information Bank Index Form

Appendix “A”

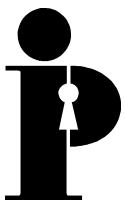
IPC of Ontario – Guidelines for Protecting the Privacy and Confidentiality of Personal Information When Working Outside the Office

Information
and Privacy
Commissioner/
Ontario

Guidelines for Protecting the Privacy and Confidentiality of Personal Information When Working Outside the Office



Ann Cavoukian, Ph.D.
Commissioner
July 2001



Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

The Information and Privacy Commissioner/Ontario gratefully acknowledges the work of Colin Bhattacharjee in preparing this report.

This publication is also available on the IPC website.

Table of Contents

1. Introduction

- In the course of performing their duties, provincial and municipal government employees may be required to work outside their employer's conventional office space. This may include transporting records by car, bus, subway, train or airplane; working on assignments or projects at home; attending meetings at hotels and conference centres; appearing at court or tribunal hearings; conducting investigations; making visits to clients or recipients of government services; and representing the government at ceremonies or public gatherings.

- Records containing personal information may be either in paper or electronic format. The purpose of these guidelines is to set out how employees should protect the privacy and confidentiality of such records when working outside the office.

2. Other Sensitive Information

- In certain circumstances, employees who are working outside the office may be dealing with other confidential records that do not necessarily include personal information, such as cabinet submissions, records subject to solicitor-client privilege, or records containing advice to government. Although these guidelines apply to personal information, they are equally applicable to records containing other types of sensitive information.

3. Freedom of Information and Protection of Privacy Legislation

- When working both inside and outside the office, government employees must comply with the *Freedom of Information and Protection of Privacy Act* and/or the *Municipal Freedom of Information and Protection of Privacy Act* (the *Acts*). One purpose of the *Acts* is to protect the privacy of individuals with respect to personal information about themselves held by government.

- Personal information is defined in the *Acts* as recorded information about an identifiable individual, including his or her race, age, family status, address, telephone number, medical or employment history and other information. Both *Acts* contain privacy rules governing the collection, retention, use, disclosure and disposal of personal information held by government. For further details, consult the full text of the *Acts*, which is available on the Information and Privacy Commissioner's Web site at www.ipc.on.ca.

4. Removing Records from the Office

- Employees should only remove records containing personal information from the office when it is absolutely necessary for the purposes of carrying out their job duties. If possible, only copies should be removed, with the originals left in the office.

- Depending on their positions, employees may be required to obtain approval from their manager before removing records containing personal information from the office.

- Records containing personal information that are being removed from the office should be recorded on a sign-out sheet that includes the employee's name, a description of the records; the names of the individuals whose personal information is being removed; and the date the records were removed.

5. Paper Records

- Paper records containing personal information should be securely packaged in folders, carried in a locked briefcase or sealed box, and kept under the constant control of the employee while in transit.

- When an employee travels by car, paper records should always be locked in the trunk. There have been cases, however, where records have been stolen from government employees, including from the locked trunk of a car. Consequently, unless there is no alternative, paper records should never be left unattended in a car trunk while the employee goes elsewhere.

- Paper records should not be opened or reviewed while travelling on public transportation such as a bus, subway, train or airplane.

- When working at home, paper records should be stored in a locked filing cabinet or desk drawer when they are not being used. The cabinet or desk should only contain work-related records.

- When working at other locations outside the office, paper records should be kept under the constant control of the employee, including during meals and other breaks. If this is not possible, the records should be temporarily stored in a secure location, such as a locked room or desk drawer.

6. Electronic Records

- Electronic records containing personal information should be stored and encrypted on a password-protected disk or CD rather than the hard drive of a laptop or home computer.
- To prevent loss or theft, a disk or CD should be carried in a locked briefcase and kept under the constant control of the employee while in transit.
- When working at home, a disk or CD should be stored and locked in a filing cabinet or desk drawer after use.
- When working at other locations outside the office, a disk or CD should be kept under the constant control of the employee, including during meals and other breaks. If this is not possible, they should be temporarily stored in a secure location, such as a locked room or desk drawer.

7. Laptop and Home Computers

- Access to laptop and home computers should be password-controlled, and any data on the hard drive should be encrypted. Other reasonable safeguards, such as anti-virus software and personal firewalls, should also be installed. Employees should only use software that has been approved by their institution's Information Technology department.
- Laptops should be kept under the constant control of the employee while in transit. When an employee travels by car, a laptop should always be locked in the trunk. There have been cases, however, where laptops have been stolen from government employees, including from the locked trunk of a car. Consequently, unless there is no alternative, a laptop should never be left unattended in a car trunk while the employee goes elsewhere.
- If it is necessary to view personal information on a laptop screen when working at locations outside the office, ensure that the screen cannot be seen by anyone else. Personal information should never be viewed on a laptop screen while travelling on public transportation.
- When working at home or at other locations outside the office, a laptop or home computer should be logged off and shut down when not in use. For added protection, they should be locked to a table or other stationary object with a security cable. To the maximum extent possible, the employee should maintain constant control of the laptop, particularly when working at locations outside the office other than home. If this is not possible, it should be temporarily stored in a secure location, such as a locked room or desk drawer.
- Do not share a laptop that is used for work purposes with other individuals, such as family members or friends.

8. Wireless Technology

- Employees should protect the privacy and confidentiality of personal information stored on wireless devices such as personal digital assistants and cell phones. Access to such devices should be password-controlled, and any stored data should be encrypted.

- To prevent loss or theft, a wireless device should be carried in a locked briefcase or closed purse and kept under the constant control of the employee while in transit. Never leave a wireless device unattended in a car. If it is absolutely necessary to view personal information on a wireless device while in public or when travelling on public transportation, ensure that the display panel cannot be seen by anyone else.

- When working at locations outside the office, the employee should maintain constant control of wireless devices. If this is not possible, they should be temporarily stored in a secure location, such as a locked room or desk drawer.

- Do not share wireless devices that are used for work purposes with other individuals, such as family members or friends.

9. Telephones and Voice Mail

- When in transit or working outside the office, employees should avoid using cell phones to discuss personal information. Cell phone conversations can be easily overheard or intercepted by individuals using scanners or other devices.

- If an employee works at home on a regular basis, a separate phone line and password-controlled voice mail box should be set up. Do not disclose the password to family members or roommates.

10. E-mail, Faxes and Photocopies

- When working at home or at other locations outside the office, employees should avoid sending personal information by e-mail or fax. If it is absolutely necessary to do so, follow the practices and tips set out in the Information and Privacy Commissioner's papers on *Privacy Protection Principles for Electronic Mail Systems*, *E-mail Encryption Made Simple*, and *Guidelines on Facsimile Transmission Security*, which are available on the IPC's Web site at www.ipc.on.ca.

- Ideally, employees should undertake the faxing or photocopying of personal information themselves. However, in some locations outside the office, fax and photocopy machines for individual use may not be readily available. If employees must submit records containing personal information to a third party for faxing or photocopying, they should ask to be present when these tasks are being done.

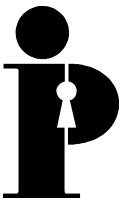
11. Conversations Outside the Office

- Employees should not discuss personal information in public locations such as buses, commuter trains, subways, airplanes, restaurants, or on the street. If it is necessary to do so, move to a location where other persons cannot overhear your conversation.

12. Reporting Requirements

- The loss or theft of personal information should be reported immediately to an employee's immediate manager, the institution's Freedom of Information Co-ordinator, and senior management. If personal information has been lost through theft, the police should be notified as well.

- The loss or theft of personal information should also be reported immediately to the Information and Privacy Commissioner, who may launch a privacy investigation, if necessary. At the outset of an investigation, the IPC may recommend that the institution notify any individuals whose personal information has been lost and take steps to contain the loss of the information.



Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

Appendix “B”

Personal Information Assessment Form

PRELIMINARY ANALYSIS QUESTIONNAIRE

1. PROJECT AND INSTITUTION

PROJECT TITLE	
INSTITUTION	
DEPARTMENT	
PROJECT LEAD	

2. PIA LEAD

NAME AND TITLE	
INSTITUTION	
DEPARTMENT	
PHONE NUMBER	
E-MAIL	

3. PROJECT DESCRIPTION

Describe the project, that is, the program, system, application or activity, that is the subject of the PIA including its purpose, scope and key objectives. Attach relevant project documentation, if necessary.

4. COLLECTION, USE AND DISCLOSURE

4.1 Identify the kinds of information involved in the project (check all that apply).

	YES	NO	UNKNOWN
Information about individuals in their personal capacity			
Information about individuals acting in their business, professional or official capacity, for example, name, job title, and business contact information			
Information about institutions, for example, for profit and not-for-profit institutions and government institutions			
Aggregated, anonymized or de-identified information. Outline in the row below the process followed to aggregate, anonymize or de-identify the information and whether it is possible to identify/re-identify individuals from that information.			

4.2 Identify the kinds of personal information that will be collected, used, retained, disclosed, secured and disposed of (check all that apply).

	COLLECT	USE	RETAIN	DISCLOSE	SECURE	DISPOSE
No personal information						
Unknown at this time (Please explain why in row below.)						
List the types of personal information involved in the project and indicate in the columns on the right whether this personal information will be collected, used, disclosed, retained, secured or disposed of. (Add rows as necessary.) If third parties will be involved in the project, think about what they may be doing with personal information as well. (Add rows as necessary.)						
List each element of non-personal information that, when combined or linked, may enable identification of an individual, and indicate in the columns on the right whether that information will be collected, used, disclosed, retained, secured or disposed of. (Add rows as necessary.)						

4.3 To whom does the personal information relate? List all the individuals whose personal information will be involved in the project, that is, the data subjects.

5. PRIVACY LEGISLATION

5.1 Identify applicable privacy legislation (check all that apply).[8]

	YES	NO	UNKNOWN
Freedom of Information and Protection of Privacy Act			
Municipal Freedom of Information and Protection of Privacy Act			
None or other (Please explain below.)			

5.2 Public Records and Excluded Personal Information[9]

	YES	NO	UNKNOWN
Identify any personal information that will be maintained for the purpose of creating a record that is available to the general public. What is the type of personal information, and why and how is it made available to the general public? (Please explain in row below.)			

[8] See the **Privacy Impact Assessment Guidelines for the Ontario *Personal Health Information Protection Act*** on how to conduct a PIA involving personal health information.

[9] Consult with your legal and privacy staff to determine if you should continue with the PIA process, and if other legislation or policies define privacy requirements that must be complied with.

	YES	NO	UNKNOWN
Identify any personal information that will be excluded from the application of the acts by section 65 of FIPPA and section 52 of MFIPPA. What is the type of personal information and why is it excluded? (Please explain in row below.)			

6. CONCLUSION

Indicate whether or not you will proceed with the PIA process and the reasons for your decision.

PROJECT ANALYSIS QUESTIONNAIRE

1. SCOPE OF PIA

Define the scope of the PIA review and analysis, that is, what aspects of the project are in and out of scope.

2. PROJECT AUTHORITY

Describe the regulatory and legal framework for the project (for example, applicable legislation and regulations, bylaws, memoranda of understandings, agreements, contracts and other relevant instruments).

3. PROJECT CHARACTERISTICS

3.1 Identify key characteristics of the project (check all that apply).

	YES	NO	UNKNOWN
Involves creating a new program, process, service, technology, information system or other type of IT application			
Involves a change to an existing program, process, service, technology, information system or other type of IT application			
Involves procuring goods or services			
Involves outsourcing or contracting for services related to the collection, use, disclosure, processing, retention, storage, security or disposal of personal information			
Involves developing a request for bids, proposals or services			
Involves a process, system or technology for which the privacy risks are not known or well documented			
Involves creating an information system or database containing personal information, and/or the matching, merging, combining or centralizing of databases			
Involves information sharing (internal and external)			
Involves the need to identify, authenticate or authorize users – public and/or internal staff			
Other activities that may impact privacy. (Please explain below.)			

3.2 If you answered yes to any of the above, explain the identified process or activity. Attach all relevant documentation to your completed Project Analysis Questionnaire.

3.3 Identify any changes that will result from the project (check all that apply).

	YES	NO	UNKNOWN
Involves a change in business owner			
Involves a change to legislative authority			
Involves a change in users (internal and external) of a related process or system			
Involves a change in partners or service providers (internal and external)			
Involves a change in the amount, type of or ways that personal information is collected, used, disclosed, retained, secured or disposed of			
Involves a change to the purposes for which personal information will be collected, used or disclosed			
Involves a change from direct to indirect collection of personal information			
Involves a change in roles and responsibilities, that is, who can do what, when, where, why and how with personal information			
Involves a change to, or elimination of, existing practices of anonymizing or de-identifying information			
Involves a change in the process or technology used to collect, use, disclose, retain, secure or dispose of personal			

	YES	NO	UNKNOWN
information, for example, hardware and software			
Involves a change to an information system or database containing personal information			
Involves a change of medium or service delivery channels, for example, the automation of manual process, conversion from paper to electronic records or the, creation of a new website to provide services to clients			
Involves a change in the security requirements or measures			
Other (Please specify change or proposed change below.)			

3.4 If you answered yes to any of the above, explain the change, that is, what specifically will change and why it is necessary. Attach all relevant documentation to your completed Project Analysis Questionnaire.

3.5 Document any additional business processes identified from your analysis of the factors identified in the guide. Attach all relevant documentation to your completed Project Analysis Questionnaire.

4. TECHNOLOGY

4.1 Identify technology-related characteristics of the project (check all that apply)**.**

	YES	NO	UNKNOWN
Involves technology designed to monitor, track or observe an individual or their transactions, for example, video cameras, cell phones and geospatial or location-based services			
Involves logging information, usage or preferences, for example, IP addresses, traffic data, access or transaction logs, cookies, or other mechanisms for recording an individual's use of technology			
Involves public-facing Internet communications, services or transactions, including websites, blogs, forums, bulletin boards, or social media			
Involves using analytics or performance measurements, for example, web analytics, social media analytics, or business intelligence tools			
Involves processing or storing of personal information in a virtual environment, for example, cloud computing			
Involves acquiring, or customizing, commercial software, hardware or IT support services by external vendors			
Involves developing, or customizing, software, hardware or IT support services "in-house"			
Involves creating information systems or other types of IT			

	YES	NO	UNKNOWN
applications that will be populated by others, for example, clients of system or service will supply information			
Involves a system or application that will automatically collect, use, disclose or retain personal information			
Other (Please explain below.)			

4.2 **If you answered yes to any of the above**, provide an explanation of the technology (that is, purposes, why necessary and how used). Include your answers to the technology questions in the guide. Attach all relevant documentation to your completed Project Analysis Questionnaire.

5. ROLES AND RESPONSIBILITIES

5.1 List other institutions or other third parties involved in developing or implementing the project and describe their role.

INSTITUTION/THIRD PARTY	PROJECT ROLE

5.2 List all institutions or other third parties that will collect, use/process, retain, store, disclose secure or dispose of personal information <u>on behalf</u> of your institution.

INSTITUTION/THIRD PARTY	RELATIONSHIP TO INSTITUTION	PROJECT ROLE

5.3 Identify any location outside of Ontario where personal information may be retained or stored and the third parties involved.

PERSONAL INFORMATION	LOCATION	THIRD PARTY

5.4 List all other parties that will have access to, or use, the personal information, for example, other program areas, IT staff, legal counsel, etc.

PARTY	RELATIONSHIP TO PROJECT	PROJECT ROLE

5.5 Identify how other institutions or third parties will be bound to follow relevant privacy and security requirements (check all that apply).

	NAME OF INSTITUTION OR THIRD PARTY	IN PLACE	BEING DEVELOPED	UNKNOWN
Contracts				
Memoranda of Understanding				
Agreements (service level and trade)				
Other (Please explain below.)				

6. RELEVANT INFORMATION

Document what and how all types of information relate to each business process and activity relevant to the project. Consider the factors identified in the guide. Attach all related documentation to your completed Project Analysis Questionnaire.

7. PERSONAL INFORMATION FLOWS

7.1 Document, in detail, the lifecycle of the personal information involved in the project in a manner that suits the project's and your institution's needs. This can be done by an information flow table or diagram. Specify the personal information involved in the project from creation and collection to final disposition. Attach any documentation needed to support your definition of personal information flow throughout the project to your completed Project Analysis Questionnaire.

PRIVACY ANALYSIS CHECKLIST

Answering the following questions can help you to identify the privacy risks that need to be addressed and the steps to be taken to ensure compliance with *FIPPA* or *MFIPPA*. You can use the table below to organize your work or it can be adapted to your own purposes and needs. Adapt to meet the needs of the project and your institution, while ensuring you address all the identified questions. Consider each instance of how personal information is involved when completing the checklist. For example, when asked about authority to collect, consider all types of personal information you will collect.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS				EXPLANATION	PRIVACY IMPACT	ACTION ITEMS
	Y[10]	N[11]	IP[12]	NA[13]			
Review each question and determine how each relates to the project. Note: Do not use the checklist as a substitute for the legislation. The statutory provisions have been summarized here.	Put a check mark (√) in the appropriate column for each question. This will create a visual representation of how the project will comply with *FIPPA* or *MFIPPA*. If your findings differ depending upon the type of personal information involved, add rows to document and explain the differences for each type.				Outline how you arrived at your findings. Provide as much information as is available, particularly if action is planned, but not yet implemented. Outline any options or alternatives that were, or need to be, considered. Explain why no action has been taken or planned for each "N" finding, and why requirements are "NA" to the project.	For each finding, outline the potential impact on privacy, for example, non-compliance with *FIPPA* or *MFIPPA*, increased intrusiveness into the private lives of individuals or it does not meet the public's expectation of privacy.	For each finding, identify the action(s) necessary for compliance with the privacy requirement or to mitigate or avoid a potential privacy impact.

[10] **Y (Yes):** You know the privacy protection requirement either has been met by existing measures or will be met by action planned before implementation

[11] **N (No):** You know nothing has been done or is planned to address this privacy protection requirement, that is, there is a possible privacy risk and "gap" in the project's compliance. If nothing has been done or planned, explain why.

[12] **IP (In Progress):** You do not know the answer to the question at this time, that is, more information or analysis is required and, until such time, there is a potential privacy risk and gap.

[13] **IP (In Progress):** You do not know the answer to the question at this time, that is, more information or analysis is required and, until such time, there is a potential privacy risk and gap.

A. COLLECTION

KEY REQUIREMENTS:

- For each collection of personal information, ensure that the institution collects personal information only if it has the authority to do so. Consider the following:
    - Is the collection expressly authorized by statute?
    - Will the personal information be used for law enforcement purposes?
    - Is the collection necessary for the proper administration of a lawfully authorized activity?
- Personal information should be collected directly from the individual to whom it relates, unless another manner of collection is authorized by the individual or statute.
- Notify the individual of the collection, including legal authority, purpose(s), and contact information of a person who can answer questions about the collection.
- See sections 28 and 29 of *MFIPPA* and sections 38 and 39 of *FIPPA*.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT	ACTION ITEMS
AUTHORITY							
Is the collection of personal information authorized under *FIPPA* or *MFIPPA* or another act?							
Do all parties collecting personal information have legal authority for the collection?							
Has responsibility for the collection been assigned to program staff or third party service providers?							
PURPOSE OF COLLECTION							
Has the purpose of the collection been defined? What is the purpose of the collection?							
NOTICE TO INDIVIDUAL							
Will notice of collection be provided to the individual(s)? Explain timing, method, and exemptions from notice, where authorized.							
Will the notice of collection comply with *FIPPA* or *MFIPPA*? Explain how or							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT	ACTION ITEMS
missing components.							
MANNER OF COLLECTION/SOURCE OF PERSONAL INFORMATION							
Will personal information be collected directly from the individual? Explain the form of collection (for example, orally, hardcopy form, online portal, etc.)							
Will personal information be collected indirectly from another source, or covertly? Why?							
Will indirect collection comply with *FIPPA* or *MFIPPA*? Explain authority for indirect collection.							
CONTROLS							
Will the project only collect personal information for which there is legal authority?							
Will there be periodic reviews of the collection controls to ensure effectiveness?							
DATA MINIMIZATION							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT	ACTION ITEMS
Is personal information necessary for the project to proceed?							
Is collection of all the personal information necessary? Why or why not?							

B. USE

KEY REQUIREMENTS:

- For each use of personal information, ensure that all parties involved in the project, for example, your institution, partners and other third parties, use personal information only with the authority to do so.
    - Is the use for the purpose it was collected or for a consistent purpose?[14]
    - Is the use authorized by the individual to whom it relates?
    - Does the use comply with another statute?
    - Is the use for other purposes permitted by *M/FIPPA*?
- See section 31 of *MFIPPA* and section 41 of *FIPPA*.

[14] A consistent purpose is a use of personal information that the individual to whom the personal information relates, that is, the data subject, might reasonably expect at the time of collection.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT	ACTION ITEMS
AUTHORITY							
Do all parties using personal information have the legal authority for the use(s)?							
PURPOSE(S) OF USE							
Has the purpose of the use been defined? Explain purpose(s).							
Will personal information be used for other purposes?							
Will uses of personal information be for purposes stated in the notice of collection or for a consistent purpose?							
MANNER OF USE							
Have all parties using personal information been defined, for example, program staff, consultants, agents, third party service providers, etc.?							
CONTROLS							
Will there be procedural, technical, and physical measures in place to ensure personal information will be used only for							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT	ACTION ITEMS
authorized purposes and by authorized parties? Explain measures.							
Will there be periodic reviews of the use controls to ensure effectiveness?							
DATA MINIMIZATION							
Is use of all the personal information necessary for the project to proceed? Why or why not?							

C. DISCLOSURE

KEY REQUIREMENTS:

- For each disclosure of personal information, ensure that all parties involved in the project, for example, your institution, partners and other third parties, disclose personal information only with the authority to do so. Consider the following:
    - Is the disclosure for the purpose for which it was collected or for a consistent purpose?[15]
    - Is the disclosure authorized by the individual to whom the personal information relates?
    - Does the disclosure comply with another statute?

[15] A consistent purpose is a disclosure of personal information that the individual to whom the personal information relates, that is, the data subject, might reasonably expect at the time of collection.

- Is the disclosure for other purposes permitted by *M/FIPPA*?

- See section 32 of *MFIPPA* and 42 of *FIPPA*.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT	ACTION ITEMS
AUTHORITY							
Do all parties disclosing personal information have the legal authority for the disclosures?							
PURPOSE(S) OF DISCLOSURE							
Has the purpose of the disclosure been defined? Explain purpose(s).							
Will personal information be disclosed for other purposes?							
Will disclosures of personal information be for purposes stated in the notice of collection or for a consistent purpose?							
MANNER OF DISCLOSURE							
Have all parties disclosing personal information been defined, for example, program staff, consultants, agents, third party service providers, etc.?							
Has the manner of disclosure been							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT	ACTION ITEMS
defined, for example, oral, mail, email, etc.?							
Will the disclosures be documented and how?							
INFORMATION SHARING AGREEMENT							
Will disclosures be documented and controlled by information sharing agreements or other means?							
CONTROLS							
Will there be controls in place to ensure personal information will be disclosed for authorized purposes, by and to authorized parties? Explain controls.							
Will there be periodic reviews of the disclosure controls to ensure effectiveness?							
DATA MINIMIZATION							
Is disclosure of all the personal information necessary for the project to proceed?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT	ACTION ITEMS
DISCLOSURE FOR RESEARCH PURPOSES							
Is it reasonably likely that personal information will need to be disclosed for research purposes?[16]							
DISCLOSURE FOR FUNDRAISING PURPOSES							
Is it reasonably likely that personal information will need to be disclosed for fundraising purposes?[17]							

D. ACCURACY AND CORRECTION

KEY REQUIREMENTS:

- Take reasonable steps to ensure personal information is not used or disclosed unless it is accurate, complete and up-to-date.
- Ensure that every individual is able to:

[16] Before such a disclosure, there should be a defined and documented process that makes sure the researcher demonstrates why identifiable information is required for the research purpose, and agrees to the terms and conditions of Ontario Regulations 460 and 823, section 10.

[17] *FIPPA* defines when disclosure of personal information by educational institutions or hospitals may be done for fundraising purposes. Before such disclosures, ensure the requirements, as defined in sections 42(2) and (3), have been met.

- correct their personal information,
- have a statement of disagreement attached to the personal information if the correction is not made and
- require a notice of the correction or the statement of disagreement to be sent to anyone to whom the personal information was disclosed within the year before the above action was taken.

- See sections 30(2) and 36 of *MFIPPA* and 40(2) and 47 of *FIPPA*.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT	ACTION ITEMS
STANDARD OF ACCURACY							
Will there be measures in place to make sure personal information is not used, unless it is accurate, complete and up-to-date? Provide details of measures.							
CORRECTING THE PERSONAL INFORMATION							
Will there be a defined and documented process for the processing of a request for the correction of personal information? Provide details of process.							
CORRECTION REQUESTS/STATEMENT OF DISAGREEMENT							
Will there be a defined and documented process for individuals to request the correction of their personal information?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT	ACTION ITEMS
Provide details of process.							
CONTROLS							
Will controls be in place to ensure that only authorized personnel will be able to add, change or delete personal information?							
Will there be periodic reviews of the controls to ensure effectiveness?							

E. SECURITY

KEY REQUIREMENTS:

- Take all reasonable measures to prevent unauthorized access to personal information in your custody or control, taking into account the nature of the record to be protected.
- Access should be restricted to only those individuals who need the personal information for the performance of their duties.
- Take all reasonable measures to protect personal information against loss or theft, unauthorized access, use or disclosure, inadvertent modification, destruction or damage, taking into account the format of the record to be protected.
- See Ontario Regulation 823, section 3 of *MFIPPA* and Ontario Regulation 460, sections 3 and 4 of *FIPPA*.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT	ACTION ITEMS
SECURITY MEASURES							
Will measures be used to secure the personal information? Explain each physical, technical and procedural measure.							
CONTROLS							
Will security policies and procedures be defined and documented to protect the confidentiality, integrity and availability of personal information?							
Will testing and periodic reviews be conducted to ensure that personal information is only collected, accessed, used, disclosed, retained and disposed of when authorized?							
Will all actions relating to the collection, use, disclosure, retention, correction, copying or disposal be logged and subject to auditing and monitoring?							
Will procedures be defined and documented on how to identify, report, investigate and address the unauthorized access, collection, uses and/or disclosure of personal information?							

F. REQUESTING ACCESS TO PERSONAL INFORMATION

KEY REQUIREMENTS:

- Ensure that every individual has a right of access to their personal information in the institution's custody or control.
- Make sure that personal information in the institution's custody or control is retrievable.
- Verify the identity of persons requesting access to their personal information.
- See section 36 of *MFIPPA* and section 47 of *FIPPA*.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT	ACTION ITEMS
ACCESS REQUESTS							
Will the management of personal information change or restrict individuals' right of access to their personal information?							

G. RETENTION

KEY REQUIREMENTS:

- Personal information should be retained for at least one year after use to provide the individual with a reasonable opportunity to access their personal information.
- The individual's consent should be obtained in order to dispose of personal information prior to one year after use.
- Ensure compliance with other relevant records retention laws, regulations, bylaws or other requirements.

- See *MFIPPA* section 30(1) and Ontario Regulation 823, section 5; *FIPPA* section 40(1) and Ontario Regulation 460, section 5.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT	ACTION ITEMS
RETENTION SCHEDULES							
Will there be defined and documented policies, procedures, and other requirements related to the retention of personal information?							
REASONABLE OPPORTUNITY FOR ACCESS							
Will measures be in place to ensure that personal information will be retained for a minimum of one year after its last use?							
MEDIUM AND LOCATION OF RETENTION							
Has the medium and format of the personal information to be retained been defined?							
RETENTION PERIOD							
If the personal information has not been used, will it be retained for only as long as necessary to meet its purpose?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
CONTROLS							
Will procedures be defined and documented related to consent for early disposal of personal information?							
Will there be periodic reviews of the retention requirements and consent procedures to ensure effectiveness?							

H. DISPOSAL AND DESTRUCTION

KEY REQUIREMENTS:

- Personal information must be disposed by either securely destroying it or transferring it to the appropriate archives.
- Make sure personal information is only destroyed when authorized by an appropriate party and in accordance with records retention regulations/bylaws applicable to the institution.
- Take all reasonable steps to protect the security and confidentiality of personal information to be destroyed throughout the process, that is, when personal information is stored, transported, handled and destroyed.
- Take all reasonable steps to protect the security and confidentiality of personal information to be transported to archives throughout the process, that is, when personal information is stored, transported and handled.
- Take all reasonable steps to destroy personal information so it cannot be reconstructed or retrieved.
- Keep an accurate record of the disposal, including what personal information was destroyed or transferred and on what date it was destroyed or transferred.
- Do not include personal information in your record of disposal.
- See Ontario Regulation 823 and section 30(4) of *MFIPPA*, section 3 of *MFIPPA* and Ontario Regulation 459 and section 40(4) of *FIPPA*.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
MANNER OF DISPOSAL							
Will procedures be defined and documented for the secure disposal, for example, transfer to archives or destruction of personal information in accordance with applicable records							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT	ACTION ITEMS
retention schedules, regulations/bylaws? Explain disposal process.							
DEVICES/EQUIPMENT							
Will procedures be defined and documented for disposal of devices and equipment containing personal information?							
CONTROLS							
Will controls be defined and documented to ensure only appropriate personal information will be disposed of or destroyed, and only by authorized parties after obtaining appropriate approval?							
Will there be periodic reviews of the disposal controls to ensure effectiveness?							
RECORD-KEEPING							
Will details of the disposal of personal information be recorded?							
Will measures be defined and documented to ensure no personal							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
information is captured in the disposition record?							

I. PRIVACY MANAGEMENT

The questions in this section relate to privacy management throughout your institution. They are not limited to the project's information system, technology or program, but address your institution's privacy maturity, capability and readiness to undertake the project. The emphasis is on accountability and training.

KEY REQUIREMENTS:

- You should apply common management principles, for example, planning, directing, controlling and evaluating the personal information collected, used, disclosed, retained and destroyed by institutions.
- Establish and follow disciplined and consistent practices for the management of personal information.
- Educate staff about privacy, as well as legislative and other relevant requirements.
- Periodically review privacy policies and practices, and commit to ongoing improvement in compliance.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT	ACTION ITEMS
ACCOUNTABILITY							
Will accountability for managing personal information throughout its lifecycle be defined to include parties involved in the project, for example, your institution, partners, vendors and other third parties? Explain accountability.							
TRAINING							
Will operational policies, procedures or practices related to the protection of personal information be needed?							
Have all parties requiring training on operational, security and privacy aspects of the project been identified?							
Has the individual responsible for ensuring that all parties receive appropriate training been identified?							
AUDITS							
Will procedures and protocols be developed and documented to evaluate whether the personal information is accessed, collected, used, retained, disclosed, secured and disposed of in a							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
manner that is consistent with *FIPPA* or *MFIPPA*?							

Appendix “C”

Personal Information Bank Index Form

Personal Information Bank Index Form

Personal Information Bank:	
Location:	
Legal Authority:	
Personal Information Maintained:	
Use:	
Users:	
Individuals in Bank:	
Retention and Disposal:	

Example:

Personal Information Bank:	Video Camera Recordings
Location:	Middlesex County Datacentre, Security Camera System.
Legal Authority:	Municipal Act.
Personal Information Maintained:	Digital images of individuals.
Use:	Passively monitor for potential security, insurance, or liability risks, the potential breach of municipal by-laws, and/or the potential occurrence of provincial or criminal offences.
Users:	Authorized personnel only as identified in the Security Camera System Policy.
Individuals in Bank:	Employees, contractors, public
Retention and Disposal	Two-weeks then securely destroyed unless retained due to a potential security, insurance, or liability risks, potential breach of a municipal by-laws and/or potential occurrence of a provincial or criminal offences in accordance with the Security Camera System Policy.