Purpose:

The Corporation of the Town of Blind River is committed to protecting personal information in the control or custody of the municipality and comply with the privacy protection requirements as mandated by MFIPPA. The purpose of this policy is to ensure that all Town of Blind River employees, members of Council, volunteers, contractors, and agents comply at all times with privacy protection requirements.

This policy confirms the Town of Blind River's obligation to protect personal information in the control or custody of the institution. Privacy breaches undermine public trust in an institution and may result in significant harm to the Town and to those whose personal information is collected, used or disclosed inappropriately.

This policy outlines the steps that shall be followed when an alleged privacy breach is reported to ensure that it is quickly contained and investigated to mitigate the potential for further dissemination of personal information.

Scope:

This policy applies to all Town of Blind River employees, volunteers, contractors, agents, and members of Council. A Procedure has been created and approved by Leadership Team.

Definitions:

"Council" means members of the Council of The Corporation of the Town of Blind River.

"Town" means The Corporation of the Town of Blind River.

"Employee" means any employee, contractors, sub-contractors and volunteer of the Town engaged in Town business, whether on a full-time, part-time, temporary or casual basis.

"Personal Information" means recorded information about an identifiable individual, including:

a) Information relating to the education or the medical, psychiatric, psychological, employment or criminal history of the individual or information relating to financial transactions in which the individual has been involved;

b) Information relating to the race, national or ethnic origin, colour, age, religion, sex, sexual orientation or martial or family status of the individual;

c) The telephone number, address, fingerprints or blood type of the individual;

d) Any identifying number, symbol or other particular assigned to the individual;

e) Correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence;

f) The personal opinions or views of the individual except if they relate to another individual;

g) The views or opinions of another individual about the individual; and

h) The individual's name if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

i) "Privacy Breach" means an incident involving unauthorized collection, use, disclosure and disposal of personal information, including it being stolen, lost, or accessed by, or disclosed to, unauthorized persons (including employee snooping or inadvertent disclosure through human error) that is not in accordance with MFIPPA.

Policy:

Protection of Privacy and Personal Information Guiding Principles

The Town is required to protect privacy and personal information to meet its legislative and corporate obligations. Protecting privacy, including the proper stewardship of the personal information and only requesting necessary personal information, is fundamental to maintaining the public's trust and confidence.

Collecting and Maintaining Personal Information

The Town will:

- collect only personal information that is relevant to and necessary for a particular purpose and will provide notice that the information is being collected. The notice shall state: the legal authority for the collection; the reason for the collection; how the institution plans to use the information; and, who to contact for more information;
- ensure all personal information collected is maintained in a secure manner;
- collect and process personal information fairly and lawfully; and
- keep personal information accurate, complete and up-to-date.

Appropriate Measures for Availability and Access

The Town will:

- make personal information available internally and externally only in appropriate circumstances (required by law or for a law enforcement purpose) or when consent by the individual has been obtained. When required by law, the Town will refer to the Information and Privacy Commissioner of Ontario's ("IPC") fact sheet, "Disclosure of Personal Information to Law Enforcement" attached hereto as Appendix A;
- only use the personal information collected for the purpose for which it was collected or for consistent purpose;
- only disclose personal information if it is permitted for the purpose of complying with law;
- provide individuals with appropriate access to personal information about themselves by providing a Freedom of Information request to the CAO/Clerk; and
- make corrections to an individual's personal information upon request to the CAO/Clerk.

Retention

The Town will:

- retain personal information for one year after it is used unless authorized under another retention period in the Town's Records Retention By-law;
- retain all personal information, whether in paper or electronic form, in a safe and secure manner.

Safeguarding Information and Privacy Breaches

The Town will:

- implement appropriate measures to safeguard personal information and instruct third parties processing personal information on behalf of the Town to process it only in a manner that is consistent with Town procedures;
- ensure that privacy protection measures are included in any contracts or agreements with third parties;
- identify and report all privacy breaches as set out in this policy;
- educate employees in privacy awareness to reduce the risk for a breach or invasion of personal information.

Protection

Employees will protect personal information from unauthorized access, loss, theft, or inadvertent destruction or damage by implementing safeguards such as:

- clean desk practices;
- lock away personal information when unattended;
- lock computer when unattended;
- lock desks and cabinets containing personal information;
- coded file labels rather than descriptive text;
- circulate personal information internally on a need to know basis; and
- security provisions in contracts with external providers of storage or disposal of records.

Roles and Responsibilities:

CAO/Clerk

The CAO/Clerk or designate shall handle all inquiries with respect to privacy breaches and the actions of the Town in response to an alleged or confirmed breach. The CAO/Clerk or designate will determine if other authorities or

organizations, such as law enforcement, privacy commissioner's office, and/or professional/regulatory bodies should be informed of the breach.

Directors and Managers

Directors and Managers shall be responsible for becoming familiar with this policy and providing training to their staff and new hires. Directors and Managers shall ensure compliance with this policy, address non-compliance and report any suspected privacy breach to the CAO/Clerk.

Employees

Employees shall:

- collect only personal information that is relevant to and necessary for a particular purpose;
- familiarize and comply with this policy, and related policies and procedures; and
- alert a Director, Manager or CAO/Clerk of a suspected privacy breach.

Procedure:

Privacy breach procedures have been created by Leadership Team and provided to all Town of Blind River employees, volunteers, contractors, agents and members of Council.

Review Cycle:

This Policy and corresponding procedure will be reviewed at a minimum of once a term of Council.

Approval Date:	February 6, 2023	Approved by:	Res #23-036
1.Amendment Date:		Approved by:	
2.Amendment Date:		Approved by:	
3.Amendment Date:		Approved by:	

PRIVACY
FACT SHEET

Appendix A

Disclosure of Personal Information to Law Enforcement

Under Ontario's access and privacy laws, institutions are prohibited from disclosing personal information, except in defined situations.

This fact sheet describes the key situations where institutions (public sector organizations such as provincial ministries and agencies, municipalities, schools, transit systems) can disclose personal information to a law enforcement agency under the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act*. It also explains how to respond when a law enforcement agency requests personal information, and how to be transparent to the public about disclosure

Generally, institutions should disclose personal information to a law enforcement agency *only when required by law*, such as in response to a court order, rather than a simple request, where there is no requirement to disclose.

However, they have the discretion to disclose in other situations, including where disclosure is made to aid an investigation, and for health or safety reasons.

In all cases, an institution should make its own careful and informed assessment of the circumstances before deciding whether to disclose personal information to a law enforcement agency. If uncertain, it should seek legal advice.

Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

SOME DEFINITIONS

Ontario's access and privacy laws define **personal information** as "recorded information about an identifiable individual." For a full explanation of the definition, see the fact sheet ***What is Personal Information?***

A **law enforcement agency** is a body engaged in policing or conducting investigations that could lead to proceedings in a court or tribunal where penalties could be imposed. Its primary function must be law enforcement (**Investigation Report I95-040P**). Other organizations that conduct investigations, such as insurance companies (**Investigation Report I95-096P**) and private security firms (**Investigation Report I95- 040P**), are not law enforcement agencies.

Institutions should make their own careful and informed assessment of the circumstances before deciding whether to disclose personal information to a law enforcement agency.

WHEN CAN INSTITUTIONS DISCLOSE PERSONAL INFORMATION TO A LAW ENFORCEMENT AGENCY?

Institutions may disclose personal information to a law enforcement agency:

1. When legally required
2. To aid a law enforcement investigation
3. For health or safety reasons

1. When legally required

In some situations, they may be *required by law* to disclose personal information, such as on receipt of a court order (search warrant or production order) (sections **42(1)(e)/32(e)** of the acts). An institution must comply with a court order unless the order is successfully challenged in court.

Institutions may be required by law to disclose personal information, such as on receipt of a court order.

2. To aid a law enforcement investigation

An institution has the discretion to disclose personal information to a law enforcement agency in Canada, without a court order, to aid an investigation (sections **42(1)(g)/32(g)** of the acts).

This type of disclosure might take place either on request of a law enforcement agency or on the institution's initiative.

On request of a law enforcement agency

After receiving a request, the institution must be satisfied that the request is:

- for specific information, **and**
- made in the context of a specific law enforcement investigation

If these conditions are met, it should then determine whether the disclosure appears likely to intrude on a reasonable expectation of privacy by considering all relevant factors, including the:

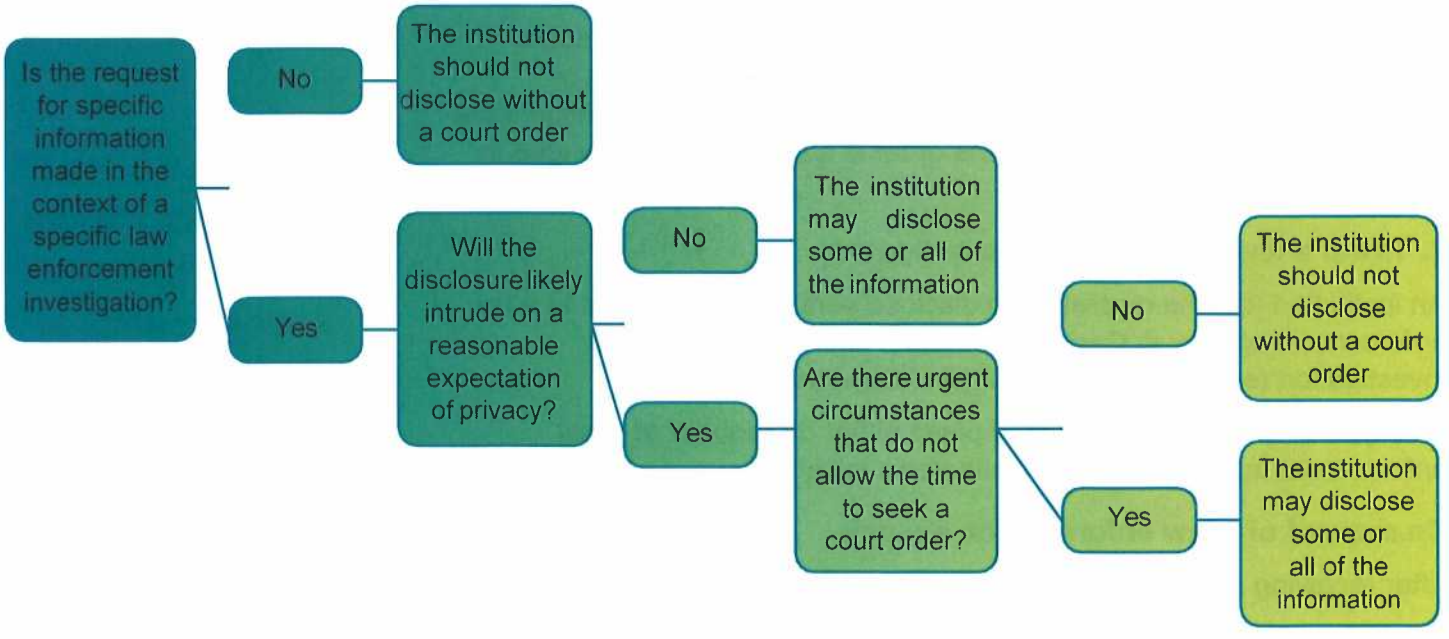
- nature of the investigation
- relevance of the information to the investigation
- sensitivity of the information
- number of individuals the information relates to
- period of time covered by the request
- number of events the information relates to

If the disclosure appears likely to intrude on a reasonable expectation of privacy, the institution should not disclose without a court order.

The only exception to this is where there are urgent circumstances that do not allow the time to seek a court order. In these cases, the institution should ask the law enforcement agency to explain why it is not feasible to seek a court order. Urgent circumstances may include cases involving a kidnapping, escaped violent offender, or missing vulnerable person.

In cases where disclosure does not appear likely to intrude on a reasonable expectation of privacy, the institution may disclose some or all of the requested information (see chart below).

LAW ENFORCEMENT INVESTIGATIONS



On the institution's initiative

An institution may disclose personal information to a law enforcement agency on its initiative, where it has a reasonable basis to believe that an offence has occurred. However, it should disclose only the information that appears to be relevant and necessary for a potential investigation. For example, if an institution captures an assault on its video surveillance system, it may disclose the video capturing the event.

If the law enforcement agency receiving the information decides not to start an investigation, the validity of the institution's decision would not be affected. What is important is that, at the time of disclosure, the institution had a reasonable basis to believe that an offence had occurred and it disclosed only the information that appeared to be relevant and necessary.

An institution may disclose personal information to a law enforcement agency on its initiative, where it has a reasonable basis to believe that an offence has occurred.

3. For health or safety reasons

An institution may disclose personal information in compelling circumstances affecting the health or safety of an individual (sections 42(1)(h)/32(h) of the acts). This includes disclosure to a law enforcement agency, whether in response to a request or on the institution's initiative.

Before disclosing personal information to a law enforcement agency for health or safety reasons, the institution must be satisfied that:

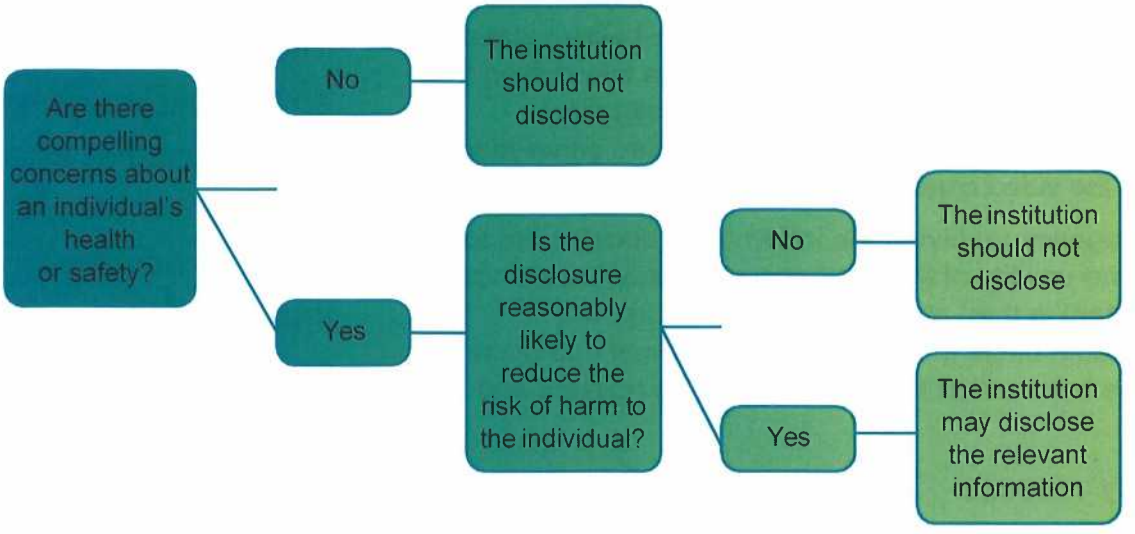
- there are compelling concerns about an individual's health or safety, having considered:
    - the likelihood of the harm occurring
    - the severity of the harm
    - how soon the harm might occur

and

- the disclosure is reasonably likely to reduce the risk of harm to the individual

If the institution decides to disclose, it should limit the disclosure to the information relevant to reducing the risk.

An institution may disclose personal information in compelling circumstances affecting the health or safety of an individual.



NOTICE OF DISCLOSURE

Under the health or safety disclosure provision in the acts, the disclosing institution *must* make reasonable efforts to notify individuals, in writing, that their information was disclosed.

In all other cases, the institution *should consider* notifying the individual. Before deciding whether to do so, it should consult with the law enforcement agency to determine whether the notice would interfere with the investigation or otherwise cause significant harm.

DOCUMENTING REQUESTS, COURT ORDERS AND DISCLOSURE DECISIONS

Institutions should document disclosure requests and court orders. An effective way to do this is to have law enforcement agencies complete and submit a form, which could include:

- the name, agency, badge number, file number, contact information, and signature of the law enforcement official seeking the information
- a detailed description of the information sought
- a description of the law enforcement purpose, investigation or proceeding to which the information relates
- the relevance of the information to the investigation
- in urgent circumstances, an explanation as to why it is not feasible to seek a court order

- the law enforcement agency's position on whether notification to the individual would interfere with the investigation or otherwise cause significant harm
- the date of the request or order

The documentation should include the decision, the name of the individual who made it, when it was made, and its factual and legal basis (for example, the specific exceptions under the acts that permit disclosure).

PUBLIC REPORTING

To be transparent and accountable to the public about their decisions, institutions should annually publish statistical information that includes:

- number of disclosures made at the institution's initiative
- number of requests received from law enforcement agencies, broken down by individual agency
- number of requests resulting in disclosure to law enforcement agencies, broken down by individual agency
- number of, and general description of the reasons for, rejected or partially rejected requests
- number of disclosures required by law, such as in response to a court order (including the law or type of court order)
- number of disclosures where there was no legal requirement to do so, broken down by those made:
    - to aid an investigation
    - for health or safety reasons
    - for other reasons, citing the specific exceptions under the acts
- number of persons whose personal information was disclosed
- a general description of the types of information disclosed
- number of individuals notified that their information was disclosed
- names of law enforcement agencies who made requests and/or received disclosures on the institution's initiative

DISCLOSURE POLICIES

The Office of the Information and Privacy Commissioner of Ontario (IPC) recommends that institutions develop and publish policies that address how they make and document decisions about disclosure to law enforcement agencies.

The IPC recommends that institutions develop and publish policies that address how they make and document decisions about disclosure to law enforcement agencies.

Disclosure policies should reflect the following best practices:

- verify the identity of the law enforcement official
- verify the authority for the proposed disclosure of personal information
- ensure that disclosure decisions are generally made by senior staff following their review of the relevant information and documentation
- where appropriate, conduct an internal review and engage legal counsel prior to disclosing to law enforcement
- take reasonable steps to ensure that the personal information is accurate and up to date
- document requests, court orders and disclosure decisions
- notify the individual whose information was disclosed, where appropriate
- annually publish statistical information on disclosure decisions

Individuals have the right to file a privacy complaint with the IPC if they believe their information has been improperly disclosed. The complaint process is described in the IPC's ***Filing a Privacy Complaint***.

For any questions or concerns about the disclosure of personal information to law enforcement agencies or the duties and obligations of institutions, contact the IPC at **info@ipc.on.ca** or 1-800-387-0073.

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

PRIVACY

Appendix B

Privacy Breaches

Guidelines for Public Sector Organizations

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

Ontario's privacy laws set out the rules for how public sector organizations should manage information about identifiable individuals — namely, personal information.

This guide explains what a privacy breach is and how to respond to one. It can also help you develop your own privacy breach response plan.

If you are an organization subject to Ontario's health privacy law, you should refer to our guidance, *Responding to a Health Privacy Breach: Guidelines for the Health Sector.*

WHAT IS A PRIVACY BREACH?

A privacy breach occurs when personal information is collected, retained, used, disclosed, or disposed of in ways that do not comply with Ontario's privacy laws. The most common privacy breaches occur when unauthorized persons gain access to personal information. For example, personal information may be seized in a cyberattack, stolen (such as through theft of a portable device) or accessed by an employee for improper purposes.

RESPONDING TO A PRIVACY BREACH

When a privacy breach occurs, you should do the following:

IMMEDIATELY ALERT APPROPRIATE PARTIES

Alert all relevant staff of the breach, including your freedom of information and privacy coordinator, and determine who else within your organization should be involved in addressing the breach.

CONTAIN THE BREACH

Identify the nature and scope of the breach and the action you need to take to contain it:

- determine what personal information is involved
- take corrective action, for example:
  - ensure that no personal information has been retained by an unauthorized recipient and get their contact information in case follow-up is required
  - ensure that the breach does not allow unauthorized access to any other personal information by taking appropriate action (for example, changing passwords or identification numbers, or temporarily shutting down a system)
  - in a case of unauthorized access by staff, consider suspending their access rights
  - retrieve hard copies of any personal information that has been disclosed

NOTIFY THOSE AFFECTED BY THE BREACH

You should notify those affected as soon as reasonably possible if you determine that the breach poses a real risk of significant harm to the individual, taking into consideration the sensitivity of the information and whether it is likely to be misused. If law enforcement is involved, ensure that notification will not interfere with any investigations.

Notification should be direct, such as by telephone, letter, email or in person. Indirect notification can be used in situations where direct notification is not possible or reasonably practical, for instance, when contact information is unknown or the breach affects a large number of people.

Notification to affected individuals should include:

- details of the extent of the breach and the specifics of the personal information that was compromised
- the steps taken and planned to address the breach, both immediate and long-term

- a suggestion, if financial information or information from government-issued documents is involved, to:
    - contact their bank, credit card company, and appropriate government departments to advise them of the breach
    - monitor and verify all bank account, credit card and other financial transaction statements for any suspicious activity
    - obtain a copy of their credit report from a credit reporting bureau
- contact information for someone within your organization who can provide additional information and assistance, and answer questions
- a statement that they have a right to make a complaint to the IPC and how to do so

INVESTIGATE

- Identify and analyze the events that led to the breach
- Review your policies and practices in protecting personal information, privacy breach response plans and staff training to determine whether changes are needed
- Determine whether the breach was a result of a systemic issue and if so, review your program-wide or institution-wide procedures
- Take corrective action to prevent similar breaches in the future and ensure your staff are adequately trained
- If you have contacted the IPC, advise us of your findings and remedial measures, and cooperate with any further investigation we undertake into the incident

NOTIFYING THE IPC

You should notify the IPC of significant breaches, such as those that may involve sensitive personal information or large numbers of individuals, or when you are having difficulties containing the breach. In these situations, you should notify the IPC as soon as reasonably possible.

In situations where you will be notifying a large number of individuals, it is important to contact the IPC before you begin the notification process, so that we are prepared to respond to inquiries.

The IPC can assist you with your breach response plan.

WHAT HAPPENS WHEN THE IPC INVESTIGATES?

When responding to a report or complaint of a privacy breach, or initiating our own investigation, we may:

- assess whether the breach has been contained and affected individuals adequately notified
- interview individuals involved
- review and provide advice on your organization's policies and any other relevant documents
- issue a report after the investigation, which may include recommendations
- issue an order

The purpose of the IPC investigation is future-oriented — that is, if there was a privacy breach, the IPC will assist the institution in taking steps to prevent similar occurrences.

HOW TO REDUCE THE RISK OF FUTURE PRIVACY BREACHES

You should consider the following measures to prevent privacy breaches:

- educate your staff about Ontario's privacy laws and your organization's policies and practices governing the collection, retention, use, security, disclosure and disposal of personal information
- conduct privacy impact assessments before introducing or changing technologies, information systems, and processes to ensure privacy risks are identified and addressed
- seek input from appropriate parties such as your legal counsel and security units, your freedom of information and privacy coordinator, the Ontario ministry responsible for information and privacy matters, and our office, as necessary

ADDITIONAL RESOURCES

The IPC has guidance that can assist your organization in meeting its privacy responsibilities and avoiding a privacy breach. You can find these documents in the guidance section of website (**www.ipc.on.ca**

About the IPC

The role of the Information and Privacy Commissioner is set out in the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act*, and the *Personal Health In-formation Protection Act*. The commissioner is appointed by the Legislative Assembly of Ontario and is independent of the government of the day.

2 Bloor Street East, Suite 1400 Toronto, Ontario, Canada M4W 1A8
Phone: (416) 326-3333 /1-800-387-0073
TDD/TTY: 416-325-7539

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario
www.ipc.on.ca info@ipc.on.ca
September 2019