

# **Shelter Management Information System (SMIS)**

## **Privacy Guidelines**

v.2

February 4, 2010



## Index

1.	Introduction	<b>3</b>
2.	SMIS Privacy Contact	<b>3</b>
3.	Definitions	<b>4</b>
4.	Notice of Collection Statement	<b>7</b>
5.	Privacy Protocol: Guidelines for Selection and Security of Passwords	<b>8</b>
6.	Privacy Protocol: Guidelines for the use of E-Mail	<b>10</b>
7.	Privacy Protocol: Guidelines for Disclosure of Personal Information to a Third Party Under Section 32	<b>12</b>
8.	Privacy Protocol: Disclosure to a Law Enforcement Agency	<b>13</b>
9.	Privacy Protocol: SMIS Interview Guidelines	<b>16</b>
10.	Privacy Protocol: Secure Disposal Guidelines	<b>17</b>
11.	Privacy Protocol: Clean Desk Policy	<b>18</b>
12.	SMIS Privacy Breach Protocol	<b>20</b>
13.	SMIS Privacy Complaint Protocol	<b>25</b>
14.	Templates	<b>26</b>

---

## **Introduction**

The City of Toronto's Shelter Management Information System is coming to your shelter in late 2009 and early 2010. This system will replace two current methods of tracking bed use in all City operated and community or purchase of service (POS) shelters in the City of Toronto: paper-based in some shelters or stand-alone systems in other shelters. Information that is entered into the SMIS system will be stored on City of Toronto servers and therefore will require that the collection, use and disclosure of this information meet the statutory requirements of the Municipal Freedom of Information and Protection of Privacy Act. In order for all staff to understand these requirements, the City of Toronto's Corporate Access and Privacy Office in cooperation with the Shelter, Support and Housing Administration (SSHA) Division are providing this training to all end users around the privacy requirements in the use of the SMIS system.

To that end this training package, in concurrence with the video developed and provided by SSHA and Corporate Access and Privacy, will provide a basic understanding and privacy protection for the SMIS end user.

## **SMIS Privacy Contact**

The SMIS Privacy Contact is a City administrator who has been trained by the City of Toronto in privacy administration and is the main contact for any SMIS end user with a privacy complaint, breach or question.

The contact number for the SMIS Privacy Contact is 416-392-8741.

---

## Definition of Terms

**Adequate Notice:** a statement that fully describes the purposes of collection, use, disclosure and retention of personally identifiable data to the individual to whom the information relates.

**Authority for Collection:** A section of an Act of Legislature, Parliament or by-law that permits the collection of personal information.

**Bare Possession:** A legal term meaning to have possession of an object or data but without ownership of the object or data.

**Business Information:** Information that relates to a business entity is specifically exempt in most cases from the restrictions placed upon personal information by MFIPPA.

**CAP/Corporate Access & Privacy:** The City of Toronto office that processes access requests and advises on privacy issues.

**Collection:** The act of collecting personal information from an individual for use in a City of Toronto program or project.

**Custody and Control:** Pertaining to information that is used by a City of Toronto division for necessary and proper functions, or is stored in facilities or information systems under the administration of a City of Toronto division.

**Data Element:** A category of data input into and moved within an information system

**Disclosure:** Any action that releases personal information from City custody and control to a member of the public or to a third party institution.

**Encryption:** A process that encodes electronic data through the use of a key and an algorithm that makes electronic data unreadable until decrypted.

**FOI:** Freedom of Information

**Indirect Collection:** Collecting personal information from a source other than directly from the individual to whom the information relates.

**Information and Privacy Commissioner of Ontario/IPC/O:** A provincial commission that acts independently of government to uphold and promote open government and the protection of personal privacy.

**Informed Consent:** The permission given by an individual for the collection, use, disclosure, indirect collection or data matching of their personal information by the City with emphasis placed on informing the individual of all uses prior to collection. It is an informed and voluntary agreement with what is being done or proposed.

---

**Implied Consent:** Consent which is not expressly granted by an individual, but logically inferred from an individual's actions and the facts and circumstances of a particular situation. (In this case, the individual's application for services under the Ontario Works Act would apply as consent to use the information provided for the provision of assistance through the shelter system).

**MFIPPA:** The Municipal Freedom of Information and Protection of Privacy Act

**Notice of Collection Statement:** A notice to an individual whose personal information is being collected by the City of Toronto that must be provided as per section 29(2) of MFIPPA. The Notice of Collection statement must include the program's authority for the collection, the specific use of the information collected and a contact within the City of Toronto who can answer questions regarding the collection and use of the information.

**Personal Information:** recorded information about an identifiable individual, including:

- information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
- information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
- any identifying number, symbol or other particular assigned to the individual,
- the address, telephone number, fingerprints or blood type of the individual,
- the personal opinions or views of the individual except if they relate to another individual,
- 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,
- the views or opinions of another individual about the individual, and
- 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.

**Public Records:** Records of personal information to which all members of the public have equal access (e.g., assessment rolls, as required by s. 39 of the Assessment Act, are public records). Please see section on "Public Records of Personal Information" for further detail.

**Unique Identifier:** A number or code that specifically relates to an identifiable individual that differentiates them from any other individual. Commonly a file

---

number is given to code an individual by an organization that collects personal information to provide a service or to determine eligibility for a program or service. Examples would include SIN numbers, Health Card numbers and application file numbers.



## Privacy Protocol: Notice of Collection Statement

According to section 29 (2) of the Municipal Freedom of information and Protection of Privacy Act, if personal information is collected on behalf of an institution, the head shall inform the individual to whom the information relates of:

- (a) the legal authority for the collection;
- (b) the principal purpose or purposes for which the personal information is intended to be used; and
- (c) the title, business address and business telephone number of an officer or employee of the institution who can answer the individual's questions about the collection.

As SMIS is collecting personal information, the following notice of collection statement must be communicated to any individual whose personal information is entered into the system.

"Your personal information is collected under the legal authority of the City of Toronto Act, 2006, Municipal Act, 2001, Chapter 169, Article VII, By-law 112-2005 and Ontario Works Act, 1997, for the purposes of administering Government of Ontario social assistance programs, providing shelter services and sharing information between shelter providers including any shelters using the SMIS system. Please be advised that the intake process will make basic personal information about you available to all linked shelters for use in ensuring the appropriate provision of shelter services and to prevent duplicate entries. Questions about this collection can be directed to the SMIS Privacy Contact, Hostel Services, Shelter, Support and Housing Administration Division, Telephone no. 416-392-8741, Metro Hall, 55 John St. 6<sup>th</sup> Floor, Toronto, Ontario M5V 3C6."

### Guidelines

- Laminate and place the notice on a card visible by the client during intake and direct their attention to it.
- During telephone collections please use the following concise version as part of your collection script if entering the information into SMIS:

"Your personal information is collected under the authority of the City of Toronto Act and is used to provide shelter services and to administer social assistance programs. Questions about this collection can be directed to the SMIS Privacy Contact at 416-392-8741."

## PRIVACY PROTOCOL: Guidelines for Selection and Security of Passwords

### Introduction

Password protection has been used for several years to control access to mainframe computer systems. More recently, passwords have also been implemented in the personal computer and local area network (LAN) environments.

Passwords help to ensure that only authorized individuals access computer systems. Passwords also help to determine accountability for all transactions and other changes made to system resources, including data.

In accordance with the *Municipal Freedom of Information and Protection of Privacy Act*, the following password guidelines have been developed to ensure that corporate business records and personal information in SMIS are adequately protected against unauthorized access.

### Guidelines

- Passwords should be kept confidential and never shared with anyone.
  - Passwords should never be written down or posted on your terminal or other obvious places.
  - Never use the same password twice. When you are selecting a password, choose one that is quite different from your previous password.
  - Passwords should be changed frequently. The shorter the life of a password, the better it is. Some systems (e.g. City of Toronto) force users to change their passwords at predetermined intervals.
  - Passwords should be a minimum of six characters in length. Weak passwords are vulnerable to password cracking utilities readily available on the Internet. Longer passwords are harder for others to guess and or crack using a commonly available dictionary cracking utility.
  - Passwords should contain a combination of alphabetic, numeric and special characters, using both upper and lower case.
  - Passwords should not be trivial, predictable or obvious.
    - **Obvious** passwords include names of persons, pets, relatives, cities, streets, your logon ID, your birth date, car license plate, and so on.
    - **Predictable** passwords include days of the week, months, or a new password that has only one or two characters different from the previous one.
-



- **Trivial** passwords include common words like 'secret', 'password', 'computer', etc.
  
- Do not use your access privileges to enable other individuals to access information that they are not authorized to access, or to submit transactions that they are not authorized to submit.
  
- Log-off when you are finished using your terminal or workstation, or if you are stepping away from your desk, even momentarily.
  
- Ensure that you activate the screensaver password protected feature (select *My Computer* and then *Display*), so that while your desk is unattended others will not be able to access your computer.
  
- Any time you suspect that someone else knows any of your passwords, change them immediately and notify your supervisor. Any misuse attributed to your password can then be investigated.

Any questions about these guidelines should be referred to the SMIS Privacy Contact at 416-392-8741.



## **PRIVACY PROTOCOL: Guidelines for the Use of E-mail**

Electronic mail (e-mail) has become an essential means of communication in the workplace. However, privacy, confidentiality and security can be seriously impacted if adequate safeguards are not followed when e-mail messages are sent and received.

E-mail messages and their attachments (printed or in electronic format) are corporate records, subject to the access and privacy provisions of the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*).

SMIS end users are responsible for using appropriate safeguards for sending and receiving sensitive personal or confidential information by e-mail.

The following e-mail guidelines have been developed for employees by the Corporate Access and Privacy Office to ensure that corporate business records and personal information in SMIS are adequately protected, in compliance with the *Act*.


### **Guidelines**

- Never send personal information derived from SMIS via e-mail
  - Keep your password confidential and change it often.
  - Before you send an e-mail containing sensitive personal or confidential information, decide if other ways to send the message would offer better privacy protection and security, e.g., a letter or memo by confidential mail.
  - Keep your e-mail user and distribution lists up-to date.
  - Verify the recipient(s)' name, title and e-mail address before you send an e-mail.
  - Do not copy e-mail messages to anyone who does not need the information to perform their job.
  - Do not forward messages you have received without the consent of the sender.
  - Use a heading that denotes your e-mail as confidential.
  - Use a subject heading that reflects the message content but does not disclose confidential information.
  - Use individuals' initials to refer to them in your e-mail, rather than identifying them by name.
-

- If you receive an e-mail intended for someone else, notify the sender and delete the e-mail immediately.
- Locate printers in secure areas.
- Pick up printed e-mails from shared printers immediately.
- Retain and file printed e-mails appropriately according to established retention schedules.
- Dispose of printed copies of e-mails in confidential waste bins or shredders, like other confidential documents.
- Send sensitive personal and confidential business information by confidential regular mail.
- Log out or use a password-protected screensaver when you leave your desk. To set-up your password protected screensaver, click on Start/Settings/Control Panel and open the folder called "Display". Click on the tab called *Screen Saver*, then choose a screen saver that you like. Then check the box called *Password protected* and indicate the number of minutes your system should wait before the screen saver is activated. Our office recommends the screen saver option be activated at 10 minutes or less.
- Report breaches of privacy and unauthorized disclosure to the SMIS Privacy Contact at 416-392-8741.

## **Conclusion**

If you have any questions about e-mail and privacy, please call the SMIS Privacy Contact at 416-392-8741.



---

## **Privacy Protocol: Guidelines for Disclosure of Record(s) in Response to a Request From an External Third Party: Section 32**

The *Municipal Freedom of Information and Protection of Privacy Act* has a series of provisions under section 32 which allow for the disclosure of personal information to outside agencies if they meet the requirements of the appropriate subsection. Please note that these guidelines are to apply to requests for information in SMIS or City operated shelters. They do not apply to records held by purchase of service (POS) shelters. In cases of requests for information held in POS shelter files, the request should be forwarded to the Shelter manager and any pre-existing protocols should be followed.

### **Guidelines**

- Refer all requests that are outside of established practices to the SMIS Privacy Contact.

In the case of an emergency, where an external third party is requesting information from a SMIS end user that will need to be provided to remove a threat to health and safety, the following protocols should be followed:

- The request must be in writing
- Proof of identity must be confirmed by checking identification, reviewing consent letters, or calling the agency to confirm the identity of the requester.
- Where possible codify frequent requests into a process that staff can become familiar with.
- All requests for information should be completed under a cover letter, the template is provided.
- A copy of the cover letter needs to be included in the client file and should also be recorded by the privacy contact.
- In all cases, if employees have any uncertainty as to the validity of the requester or of the circumstances they are to refer the request to the Privacy Contact except in cases of emergencies that threaten health or safety.



## Privacy Protocol: Guidelines for the Disclosure of Personal Information in Response to a Law Enforcement Request under MFIPPA or PHIPA

### Introduction

One of the key principles of the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) is the protection of personal information. The requirements of these acts concerning personal privacy include establishing standards for the collection, use and disclosure of personal information.

“SMIS client files” includes records that are considered personal information. Shelters frequently receive requests for access to this information from a variety of external government law enforcement agencies, including City of Toronto Police Services (TPS), the Ontario Provincial Police (OPP) and the Royal Canadian Mounted Police (RCMP).

The collection, use and disclosure of personal information (other than personal health information) are restricted to specific circumstances outlined in Part II of the MFIPPA. Section 32 (g) of MFIPPA permits the disclosure of personal information by the City of Toronto to a law enforcement agency in Canada for the purpose of aiding an investigation undertaken with a view to a law enforcement proceeding.

The City of Toronto, Corporate Access and Privacy unit has developed a corporate form and these guidelines to assist City staff in identifying when they are permitted to disclose personal information in response to a request received from a law enforcement agency in Canada, and specific procedures to follow when disclosing personal information in these circumstances.

Please note that these guidelines apply to requests for information in SMIS or City-operated shelters. They do not apply to records held by POS shelters. In cases of requests for information held in POS shelter files, the request should be forwarded to the Shelter manager and any pre-existing protocols should be followed.

### Guidelines

- Refer all requests of this nature to the SMIS Privacy Contact. If the request is an emergency that is deemed to have potential impact upon health and safety and the privacy contact cannot be contacted, the following guidelines should be used prior to any disclosure of information to a law enforcement officer.
    - When a law enforcement officer attends at any SMIS-enabled facility requesting access to personal information in SMIS, they must complete a Law Enforcement Officer’s Request for Access to Personal Information form (Attached).
-

- Staff are required to ask the attending police officer for identification and ensure that their badge numbers are recorded on the form.
- Staff are to complete Part I of the forms, indicating whether the request is for employee or client information, the location, the file title and a brief description of the records requested by the police.
- If the information requested is personal health information, staff must determine whether disclosure is permitted in accordance with the criteria listed on the previous page. If not, the request must be refused, and the police should be referred to the City's Corporate Access and Privacy Office.
- For personal information other than personal health information, staff can assist the police in identifying in detail what information they require, so that only these records relevant to the investigation are disclosed. In the event that specific information cannot be identified, but the police are requesting to search through large volume of records, please contact the Corporate Access and Privacy office for further direction.
- Part II of the form is to be complete by the attending police officer. He/she must record:
  - An occurrence report number
  - Whether copies are requested or to view the original, or both
  - Whether the originals will be requested under subpoena

Note: Originals are never to be provided to an attending officer.

- Staff must ensure that the forms is dated and signed by the requesting officer and attending staff person.
  - **Forward the completed original form in a sealed envelope, marked confidential to the SMIS Privacy Contact.**
  - Place a copy of the completed form, along with copies of the records that were disclosed to the law enforcement officer, in the employee or client file.
  - If presented with a subpoena, you will likely be expected to attend at court with a certified copy of the original records that have been requested. Staff must contact the shelter's solicitor when presented with a subpoena.
  - **Special Note:** There may be exceptional circumstances that arise in which staff receive a request from the police for information over the telephone. Please refer all such calls to the SMIS privacy contact prior to disclosing any personal information.
-

Copies of the form can be obtained from the Corporate Access and Privacy office by calling 392-9684. Any questions related to these guidelines can be directed to the SMIS Privacy Contact at 416-392-8741.



## **Privacy Protocol: SMIS Interview Guidelines**

SMIS clients are required to disclose personal information during multiple interviews at intake and in program areas.


The information collected during these interviews and examinations potentially involve sensitive personal information. The SMIS interview guideline has been drafted to assist staff in providing the best possible protections for client information during the interview process.

### **Guidelines**

- In all cases staff should attempt to conduct interviews in the most secure area possible.
- When using a less than private area, common room or open interview area, staff should attempt to conduct the interview in as secure a manner as possible by asking occupants to leave or otherwise securing the area.
- In all cases clients should be informed that they have the right to wait for a secure interview area if they do not wish to have the interview conducted in a common area.
- Employees who are collecting information in common areas must be mindful of the amount and type of information collected and if possible ask for the minimal amount of information possible in the circumstance.
- In circumstances where interviews may be conducted in a common area with a greater possibility of eavesdropping, SMIS end users should ensure that the following permissions are completed by staff:
  - Client has consented to the interview in the common area
  - Client is incapable physically of being moved into a secure interview area
  - Employee health and safety is at risk.

### **Conclusion**

Employee questions regarding the SMIS Interview Policy can be directed to the SMIS Privacy Contact at 416-392-8741.



---



## **Privacy Protocol: Secure Disposal Guideline**

Many of the documents produced in SMIS contain personal information. It is strongly recommended that any printing of hard copy records from SMIS be minimized. Any information that is printed for inclusion in hard copy files needs to be securely and responsibly managed. All documents of this sort must be disposed of in a secure fashion when it is no longer used in shelter files. All print copies, accidental or purposeful must be disposed of using the SMIS disposal guideline (outlined below). SMIS is responsible for safeguarding the information within any document produced during any client relation for the entirety of the document life cycle.

### **Guidelines**

Any document of any sort with a client name on it should always be disposed of using the following guidelines:

- Any document containing personal information or personal health information must be disposed of in a locked secure disposal bin or by shredding.
- Secure bins must be emptied before the documents inside reach a level where they can be removed through the disposal opening.
- Shredders should be placed close to the SMIS monitors for ease of staff use.
- In cases where a secure bin is not feasible and a shredder is not present, a separate receptacle for sensitive documents should be placed in a secure location and emptied at the end of each shift into either shredder or a secure bin.
- Never dispose of document containing personal or personal health information in recycling bins or in the regular garbage.

Any questions regarding the secure disposal of documents or to requisition a red bin or shredder, contact the SMIS Privacy contact 416-392-8741.



## **Privacy Protocol: SMIS "Clean Desk" Information Practices /Working Area Guidelines**

### **Introduction**

In the past decade there has been considerable focus upon corporate privacy and security involving documents containing personal information (documents). This focus has raised awareness of the potential for unwanted disclosure of documents in the electronic transmission and storage of personal information.

Staff should be aware that the electronic/physical storage and in-office use/review of these kinds of documents can have serious implications for privacy, confidentiality and security.

The Corporate Access and Privacy Office has developed a set of guidelines that can assist staff in adopting a "clean desk" policy that will ensure compliance with privacy legislation.

### **Guidelines**

- Follow the password protocol and guideline
  - When leaving your workspace for a short period of time when reviewing documents, move the records into a position where they are not visible to people walking by. Place them into a drawer, a closed filing cabinet or an equivalent while you are away. If you work in an office with a door, close it.
  - Absences of a longer period should have the documents placed in a secure area for the duration of your absence. (e.g. locked desk drawer or office, filing cabinet.)
  - At the end of a working day, all documents should be returned to a locked filing cabinet or an equivalent and the keys removed from obviously accessible areas. SMIS terminals should be signed out and or turned off if use is completed for the day.
  - Never leave documents unattended at photocopy machines or in other areas with multiple staff access. Remember to check copying machines and printers for duplicates and to ensure no originals have been left inside the machine.
  - Empty your wastepaper basket at the end of each day. Please ensure that shredding or an equivalent method disposes of any unwanted copies of documents.
  - Set your desktop computer to time-out to a screen saver for the minimum reasonable time after use. The screensaver should be password protected requiring the user to sign on to regain access to the computer.
-

- Be aware of the placement of your computer screens to prevent information from being displayed insecurely. Shift your monitor to avoid "shoulder surfing" and do not place a terminal in a common area where the public can access it.
- Review the storage of information within your physical work area for security and privacy
- When fielding a request for confirmation as to the attendance of an individual within the shelter system the following process should be undertaken:
  - Record the contact information of the caller/requester
  - DO NOT confirm or deny the client's presence in the shelter or the system
  - Inform the requester that IF the individual is in the system that the contact information will be passed along to them and they will decide whether or not to contact the requester
  - Please remember that even confirming the presence of the individual within the shelter system is a breach of their confidentiality and personal information.
- The posting of information derived from SMIS in common areas should be avoided.

## **Conclusion**

These guidelines, in conjunction with staff awareness of their roles in maintaining a privacy-conscious workplace, will assist in meeting the requirements of the *Act* and protect the client from inappropriate disclosures of their information.

For more information about this policy contact the SMIS Privacy Contact at 416-392-8741.

---

# Privacy Breach Protocol

## Background

SMIS end users are engaging in the use of a system that falls under the statutory requirements of the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA). As such, it is a legal requirement under Section 1.b of MFIPPA that the personal information collected and used by the institution is safeguarded against inappropriate and/or negligent disclosure.

Personal information is recorded information about an identifiable individual. The SMIS Privacy Breach Protocol is a set of guidelines that outline the process to be followed in the event of a privacy breach involving SMIS information assets. The protocol has been developed by the City's SSHA Division and Corporate Access and Privacy for the SMIS end user.

## Privacy Breach

A privacy breach is any instance where an institution allows intentionally or unintentionally the disclosure of personal information or records containing personal information. Examples can include a lost or stolen computer or peripheral device or the mailing of sensitive information to the wrong address. In the case of SMIS it could include the system being hacked by an outside user, or the printing of client files which are then lost or stolen.

Privacy breaches undermine public trust in an institution and can result in significant harm to the City, the shelter and for the individuals to whom the personal information relates. In all cases the resolution and mitigation of a privacy breach is to be considered as the highest priority for all City staff.

## Protocol

When a privacy breach involving the SMIS is discovered, immediate action should be undertaken by shelter staff. The following protocol should be followed in all instances.

### Step 1: Confirm

Confirm that a privacy breach has occurred. If a breach has taken place a supervisor or shelter manager should immediately assess the circumstances of the breach.

The supervisor (or the shelter's SMIS Access Manager) will be responsible for contacting the Privacy Contact within 24 hours of the breach, who will then advise on the process.

The SMIS Privacy Contact will be responsible for:

---

- All documentation of the particulars of the incident
- Contacting the Corporate Access and Privacy (CAP) unit
- Coordinating the reporting of specifics relating to the incident by shelter staff
- Providing divisional policies and case files relating to the incident
- Being the point of contact for any mitigation strategies developed in response to the circumstances of the breach
- Suspending any processes deemed to be responsible for the breach if on-going

## Step 2: Contact

All contact provisions in the case of a privacy breach must be completed within 24 hours of discovery. (If during assessment, the breach can be remediated or resolved then the following processes do not need to be completed. Breaches that involve any high risk information should follow the guidelines.)

Ensure appropriate staff are immediately notified of the breach, including:

- The Corporate Access and Privacy Office
- The SMIS Privacy Contact
- SSHA Divisional IT Manager
- Other appropriate staff

These individuals will form the core of the Privacy Breach Response Team (PBRT).

The PBRT is required to hold a telephone conference call for information and mitigation purposes as soon as it can be arranged. This should occur no later than 48 hours after the breach has been discovered.

The PBRT will need to be notified of all particulars relating to the incident including:

A detailed record of the occurrence and the steps taken to that point arranged chronologically using the attached briefing note template.

In most cases the breach will need to be reported to the Information and Privacy Commissioner (IPC) of Ontario. The CAP office will be the **only** point of contact for this notification. **Under no circumstances should shelter staff contact the IPC.**

## Step 3: Contain

The Shelter Operator in cooperation with the SMIS Privacy Contact must immediately:

- Suspend any process that caused the privacy breach if this behaviour is on-going.
  - In cases where the breach is due to the theft of equipment — police must be notified and a police report filed immediately.
  - In cases where the occurrence is a single unrepeated error (a stolen computer or single mis-mailing)— all policies relating to the occurrence will need to be reviewed
  - In cases where the breach is as a result of an on-going practice, operations involved in
-

- The privacy breach will be suspended until it is resolved.

If possible, with the cooperation of the CAP office, the lead contact in the shelter should immediately move to retrieve any documentation that has been disclosed inappropriately with all actions documented.

#### **Step 4: Investigate**

The PBRT should be informed of all policies/procedures or staff actions that precipitated the privacy breach. These should be used to develop the mitigation of the breach to be undertaken by the area. Breaches that are reported to the IPC will require a detailed submission including the above information. Assigning these responsibilities is integral to successfully mitigating the breach and preventing recurrence of the circumstances responsible for it.

#### **Step 5: Document**

Using the attached briefing note, the shelter operator collects and arranges all information pertaining to the privacy breach. This information will include:

- The date, time, place and material involved in the breach
- A chronology of steps including notice
- Staff identified by position in the body of the briefing note with an appendix listing the names and positions mentioned in the note itself
- The scope of the breach—the number of individual records involved
- The nature and sensitivity of the information disclosed
- Any policies or procedures responsible for the breach
- Any attempts at mitigation undertaken to-date

#### **Step 6: Mitigation**

The PBRT should meet to discuss mitigation of the event. Mitigation may involve the retrieval of the information where possible, the revision of policies and procedures in place and the suspension of processes until subsequent breaches are prevented.

Common mitigation strategies will involve:

- re-education or training for staff members involved
- mailing of notice letters to individuals directly affected by the breach
- altering or adjusting pre-existing policies
- retrieval of the record or information, where possible
- In these cases the shelter contact will need to appoint a telephone contact for inclusion in breach notice
- letters to allow affected individuals contact within the division for updates and follow-up on the breach mitigation process.

The SMIS representative in the City's Legal Services Division should be notified along with the lawyer for the shelter in the case of a breach at a community based shelter and mitigation strategies should be assessed prior to implementing notification.

---

In cases where the IPC has been notified of the breach, all mitigation strategies will need to be detailed in the official submission.

Privacy breaches are a very serious matter. The City of Toronto privacy breach protocol will minimize and mitigate the potential harms resulting from them.

The Privacy Contact uses the attached briefing note as a template for developing the initial report to the CAP office and the PBRT. The City's Corporate Access and Privacy Office may be contacted to provide advice at any time during this process.

## **Privacy Breach Briefing Note**

**Date of Privacy Breach:**

**Date Reported to CAP/ PBRT:**

**CAP Representative's Name:**

**Division and Section Name:**

**Division Contact's Name:**

**Position Title:**

**Address:**

**Telephone Number:**

**Email address:**

**Summary of privacy breach (who, what, when, where, why and how):**

**Was a third-party involved (e.g. an organization providing services under contract with the City)?**

**Summary of Issue and Action Taken:**

**Investigation details**

**Containment Efforts (what efforts (if any) were made to control the breach)**

**Consultation with City's Corporate Access and Privacy Office (CAP)**

**Representative Future Action/Follow Up:**

**Appendix 1: Staff Members Directly Involved**

---



# SMIS Privacy Complaint Guideline

## Introduction

A SMIS client has the right to complain about any practices involving their personal information that they feel is unlawful or in any way questionable.

All complaints relating to the inclusion of their information in SMIS should be taken seriously.

Please follow the guidelines to ensure that the complaint is recorded and addressed. Formal complaints by SMIS clients to the Information and Privacy Commissioner may place the system at risk and should be avoided if possible by attending to the complaint as quickly and efficiently as possible.

## Guidelines

- Record the name, date, time and substance of the complaint as well as the name of the staff member who took the initial complaint.
  - Inform the shelter manager or designate of the complaint.
  - Contact the SMIS Privacy Contact within 24 hours of the occurrence.
  - Cooperate with the investigation of the complaint.
  - Implement any recommended amendments to the processes in a timely fashion
-

# Templates

## Template: Disclosure letter for section 32 (e) requests

<<Date>>

<<Name of Investigator>>

<<Title of Investigator>>

<<Organization>>

<<Address>>

<<City, Province>>

<<Postal Code>>

Dear (Mr./Ms.) <<Investigator Name>>,

Re: <<Subject of Request>>

I am replying to your letter of <<date>> requesting information related to the <<specific document description>> of the above named individual from the <<Division >> of the <<Department>>.

Please be advised that the specific personal information that has been requested is being disclosed pursuant to the <<cite the requesters specific legal authority (e.g. *Income Tax Act*)>>, <<section/subsection/chapter>>. This disclosure is permitted by section 32 (e) of the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*) which permits an institution to disclose personal information for the purposes of complying with an Act of the Legislature.

Please find enclosed a copy of the records responsive to your request maintained by the <<Division>> of the <<Department>>.

Should you have any questions related to this release of information please contact the Department contact with the City of Toronto at (416) 39x-xxxx.

Sincerely,

<<Manager>>

<<Title>>

<<Division>>

---

**Template: LAW ENFORCEMENT OFFICER REQUEST FORM: ACCESS TO PERSONAL INFORMATION**

The following information is being requested under section 32(g) the Municipal Freedom of Information and Protection of Privacy Act which provides for the disclosure of records containing personal information for the purpose of aiding a law enforcement investigation.

*This section to be completed by Shelter Staff:*

Information Requested

File Description:

File Location (Area/District Office):

File/Record Title(s):

Description of Records:

*This section to be completed by attending Law Enforcement Officer (including: Toronto Police Service, OPP, RCMP, Correctional Service of Canada, Ontario Ministry of Correctional Services).*

Record Description:

Subject Name:

Occurrence No. \_\_\_\_\_ or Warrant of Apprehension No. \_\_\_\_\_

Review Original Documents: Yes  No  Copies Requested \_\_\_\_\_

Original Requested:

(release original under subpoena only)

I \_\_\_\_\_ request the above personal information to aid an investigation undertaken by \_\_\_\_\_ with view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result.

\_\_\_\_\_  
*Signature of Investigating Officer*      *Badge/Identification No.*      *Date*

\_\_\_\_\_  
*Signature of Staff Member*      *Date*

Shelter contact name: \_\_\_\_\_ Phone #: \_\_\_\_\_

SMIS End Users must return all completed ORIGINAL forms to the SMIS Privacy Contact at: Hostel Services, SSHA Division, 6<sup>th</sup> Floor, Metro Hall, 55 John St., Toronto M5V 3C6.