June 4, 2010

Hostel Services Guideline – *Shelter Management Information System (SMIS) Implementation* - 2010 – 34

HS Guideline Number:	***2010 - 34***
Date Issued:	June 4, 2010
Last City Guideline Received:	Shelter Management Information System (SMIS) *2009-33-Revised Interim Per Diem & Personal Needs Allowance Submission Claim*
Subject:	SMIS Implementation
Effective Date:	1st Day of SMIS Go Live Date
Applicable to:	The policies and procedures in this Hostel Services Guideline apply to all shelter operators that went live in SMIS since its implementation in the fall of 2009.
Who To Call for Information:	Agency Review Officer

Background:

The Shelter Management Information System (SMIS) is a web-based information management system for City of Toronto funded shelters serving homeless families, singles and youth. SMIS automates manually-intensive work practices, increases the efficiency of managing and administering the Toronto shelter system, and supports day-to-day shelter operations more effectively, thereby providing more responsive and coordinated client services in all shelters across the City.

SMIS streamlines client Intake, Admission and Discharge. It also provides the following features: manage bed occupancy, view real time occupancy across the shelter system, facilitate referrals, support case management, view client history, manage complaints, service restrictions and incidents, flag health and safety restrictions, automatically provide client's current status in Ontario Works (OW) and/or Ontario Disability Support Program (ODSP) to assist shelter staff with determining clients' Personal Needs Allowance (PNA) eligibility, and produce a wide range of reports.

At this time, SMIS will not handle any billing or PNA pay-out functions, but will be able to generate reports with information required to assist with the calculation and reconciliation of the monthly per diem billing submission and the calculation of PNA to eligible residents. Full billing and PNA pay-out functions will be part of a future module.

This Hostel Services Guideline is one of a number of guidelines you will receive related to the implementation and use of SMIS.

As a condition of the operating agreement with the City, all agencies are required to put processes in place to meet the following requirements and responsibilities related to SMIS. For further details and additional requirements and responsibilities, agencies are to refer to Schedule C of their 2010 Operating Agreement with the City.

SMIS REQUIREMENTS & RESPONSIBILITIES:

1. Data Entry Requirements

SMIS features "real-time occupancy", which means that at any time of day or night, shelter staff and Hostel Services can see how many available beds are in the shelter system and where those beds are. This feature is available through the Referral screen and in some cases through reports.

Accurate and up-to-date real-time occupancy numbers are critical for three reasons:

(1) Any shelter staff making a client referral to another shelter can view the actual vacancies in another shelter in order to provide appropriate service to the client;
(2) Hostel Services requires real-time occupancy information for various reporting purposes; and,
(3) Agencies need to generate reports on actual bed occupancy within a specified time frame to assist with the calculation and reconciliation of monthly per diem billing submission to Hostel Services and the calculation of Personal Needs Allowance to eligible residents.

In order to maintain accurate up to date bed occupancy information, **entries must be made in real-time**. Therefore, shelter staff must:

(1) enter the **Intake and Admission** into SMIS **immediately** upon assigning a bed or room to the client/family. The system will prompt the User to fill in all mandatory fields marked with an asterisk (*). An Overnight Pass is to be issued if required.
(2) enter the **Discharge** information into SMIS **immediately** upon a client/family is discharge.

Failure to follow this procedure will result in inaccurate real-time occupancy reports, potential misdirected referrals and inaccurate occupancy (i.e. actual bed nights) information for per diem and PNA billing calculation & reporting purposes.

2. Maintenance and Support

a) City Responsibilities

The City will maintain all data in a centralized secure server. The database is backed up every day by the City's Information and Technology Division staff. All data will reside **only** in this centralized database.

The City's Shelter, Housing and Support Division (SSHA) staff will provide technical support to SMIS through a SMIS Help Desk. The Help Desk is a centralized access point for all SMIS Users and can be accessed via telephone and/or e-mail.

The Help Desk hours of operation, phone number and e-mail address are as follows:

Hours of Operation: *(subject to change)*	7 a.m. to midnight (seven days per week)
Phone Number:	416-397-SMIS (7647)
Help Desk E-mail:	smishelp@toronto.ca
Assistance Outside of Help Desk Operating Hours:	Any SMIS users requiring technical assistance outside of the Help Desk operating hours can leave a voice mail message or send an e-mail to the SMIS Help Desk.

Prior to SMIS implementation, City staff installed a 'certificate' of access to SMIS on each computer that was identified by shelter operators to be used for SMIS. No other computers shall access SMIS.

The certificate will help ensure secure access to SMIS and is **NOT** to be altered or duplicated. Refer also to section 2 (b) (iv).

The City is responsible for all upgrades and enhancements to the SMIS application.

b) Agency Responsibilities

The Agency shall:

i. Retain ownership of and at all times maintain in good operating condition all hardware required for SMIS.
ii. Ensure physical security of all hardware (i.e. computers, mouse, client signature pads, scanner, etc) used in relation to SMIS.
iii. Replace hardware when required, at the shelter's expense. This includes the client signature pad, its batteries and the scanner.
iv. Notify the City regarding the acquisition of new and/or disposal of old C-drives and/or computers used to access the SMIS application in order for City staff to install or remove certificates of access to SMIS.
v. Maintain updated anti-virus/anti-spyware software and ensure that, at minimum, a weekly virus scan, automated if possible, is performed.
vi. Maintain high-speed internet access.
vii. Cover any other costs associated with moving, replacing or updating hardware.

3. User Responsibility and Confidentiality Agreement

Every person that is required to use SMIS as part of their work (the "User") must sign a User Agreement (see attached Appendix 1) in order to be issued a SMIS UserID and Password from the City.

The Agency shall ensure that each user sign a User Agreement and keeping the signed original copy on file at the shelter. All completed and signed User Agreements must be scanned and e-mailed to smishelp@toronto.ca. Faxes will not be accepted.

The Agency will ensure that user obligations related to SMIS are clear to each staff and that the agency has provisions in place in the event that the employee violates the obligations.

4. SMIS Access Manager and Alternate & User Names, Roles and Access Rights

Prior to implementation, each Agency was asked to provide the names, roles and required access rights for each user in their shelter (for example, front-line, case worker, supervisory access rights). Based on the information provided and following user training and submission of signed User Responsibility and Confidentiality Agreements, the City's SSHA Division assigned user access rights to SMIS. Prior to implementation, the user access rights information was sent to the Agency for sign-off.

For security, privacy and confidentiality reasons, any persons or students (as part of their student practicum/placement) providing volunteer work or help at any of the shelter sites are not to be given access rights to the SMIS application. The City does not have the resources to provide support to any request or maintain a student user's access rights information given the short term and frequent turn over of their volunteer work/student placement assignments.

Any new requests and/or changes to SMIS UserID, roles and access rights must be submitted by the shelter site designated "SMIS Access Manager" or Alternate to the SMIS Help Desk. They are the ONLY authorized staff to sign off on SMIS User Roles. SMIS Help Desk will not process any request and/or changes from any other shelter staff. All changes (additions and deletions to staff/users, as well as changes to staff access rights to SMIS) must be submitted within 24 hours, using the SMIS User Access Request Form, so that the City can maintain updated access levels to the system.

Access to SMIS will only be granted to a User when the SMIS Help Desk has received the signed User Agreement and the User Access Request form.

Further details of the role and responsibilities of the "SMIS Access Manager" and the Alternate are detailed in Schedule "C" of each of the Agency's 2010 Operating Agreement with the City.

Schedule "C", Section 3.1 of the Operating Agreement refers to the Access Manager as "responsible for liaising with the City with respect to all matters related to the System and responsible for managing the transfer and sharing of all System Information between the City and Agency." While this role may evolve over time, two initial priority tasks are as follows:

(i) Communications

The Access Manager and Alternate will be the primary of contact for any items, except for any per diem and/or pna billing matters, related to SMIS:

a) From SSHA to the shelter (for example updates on SMIS, new release notes, training information, Guidelines, other follow-up). This person will forward any SMIS-related information to the appropriate parties at the shelter, as required.

b) From the shelter to SSHA (for example requests for merging client files, training registrations, and other requests).

(ii) Quality Control

This position will be responsible for contacting SMIS Help Desk with requests for merging duplicate client files arising from his/her shelter and for following up with Users who create the duplicate files. Any reports produced by SSHA about duplicate files will be sent to the Access Manager or Alternate, who will be expected to follow up with corrective action.

The Agency shall ensure that their designated authorized "SMIS Access Manager" and Alternate remains current. Any changes to the agency's SMIS Access Manager or Alternate must be sent by the Executive Director by e-mail to the SMIS Help Desk (smishelp@toronto.ca).

The shelter's designated Access Manager is **not** responsible for resetting passwords. SMIS users are responsible for notifying the SMIS Help Desk if they are locked out of the system or if they believe their password has been compromised, in order to receive a new password. A new password can only be issued by the City.

5. Confidentiality and Privacy

Section 5.0 of Schedule C in the 2010 Operating Agreement details the Agency's role and responsibility on the confidentiality and privacy of "Required Information" in SMIS. As per Schedule C, "Required Information" means "any information input into the System (SMIS) to which the City has access and which the City requires for the purposes of carrying out its business with the agency and which is otherwise required for the purposes of the System."

Under confidentiality and privacy, the Agency's responsibility includes its obligation to read and/or provide the Notice of Collection to each client from whom any "Required Information" is collected, prevent the unauthorized or inadvertent use of the system, disclosure, loss, alternation or destruction of "Required Information", and compliance with the Breach Protocol and the requirement to notify the City immediately of any potential or actual breach.

The City developed a SMIS Privacy Guideline and DVD, which were provided to all agencies at several training sessions held in February and March of 2010. Each agency was provided copies of the guideline and DVD as a reference and training material for staff. The guideline includes a privacy breach protocol, which details the reporting process involved when a privacy breach has been discovered, and the role and responsibilities of the SMIS Privacy Contact and Agencies. All SMIS users are required to become familiar with and trained on the guideline. Agencies shall ensure that the dates of the training are logged and kept on site. See Appendices 2 to 5 of this Guideline for SMIS privacy related protocols, guidelines, notice of collection and templates.

Where a Privacy Breach has occurred, the Agency is responsible for informing the SMIS Privacy Contact within 24 hours of the breach.

6. System Unavailable: Continuity of Operations

The Agency is responsible for ensuring that all staff are aware of the manual back-up process in case of system interruptions (e.g. power failure or internet access failure). The City has supplied electronic forms of all input screens of SMIS and the Agency is responsible for saving these in the

network or hard drive and for printing copies and ensuring that they are available for use as required.

The Agency will ensure that hard-copy forms are appropriately used while the system is down. The City will work with Agencies to ensure that clients are admitted into SMIS when the system becomes available.

7. Shelter 'Tombstone Data' (All Levels)

Each shelter's basic organizational information (i.e. name, address, funded beds, etc.) has been entered into the system. This information was signed off by the Agency before the shelter first 'went live'. The Agency (i.e. the Access Manager) will be responsible for notifying the SMIS Help Desk and their assigned Agency Review Officer of any and all changes to the tombstone data of the shelter, so that the City can maintain up-to-date information in the system. Changes include additions, deletions and revisions at the level of the organization, shelter, facility, or program (including but not limited to contact information, address or program changes).

8. Reports

a) Resident Bed Log

As per the Toronto Shelter Standards, (Section 3.3 – Financial Accountability), all agencies are required to maintain a resident bed log for a minimum of seven years for financial audit purposes. All agencies are required to print the **SMIS Bed Log** at the time of final bed count, which must fall between the hours of 2:00 a.m. and 4:00 a.m. The staff person conducting the bed check and completing the SMIS Bed Log must print their name, time of bed count and sign the sheet as well. The completed and signed SMIS Bed Log must be kept on file on site for a minimum of seven years.

b) Weekly Occupancy Form

All agencies are to continue using the Weekly Occupancy Form and submit it to Hostel Services until September 1, 2010. The City is working on developing a report in SMIS to produce the information captured in this form.

c) Monthly Service Restriction Report

All agencies are no longer required to use and submit this form to Hostel Services as the information can be generated from SMIS.

d) Monthly Service Request Reporting Form

All agencies are no longer required to use and submit this form to Hostel Services as the information can be generated from SMIS.

9. Residents' OW/ODSP Status

Residents' benefit status in OW/ODSP will soon be available in SMIS in order for shelter staff to determine each resident's eligibility for Personal Needs Allowance. The City will notify all agencies once this information becomes available in SMIS and a guideline will be issued to assist staff with

interpreting the information provided. Until then, agencies are required to check residents' OW/ODSP benefit status as per current practices.

10. Interim Per Diem & PNA Billing Submission

An interim per diem and PNA billing submission guideline and forms (see Hostel Services Guideline -SMIS Interim Per Diem & PNA Billing-2010-33) was developed and the last version was issued to all agencies in April 2010. All agencies are required to adhere to the guideline and use the new billing forms for submission to smisbill@toronto.ca.

ACTION REQUIRED BY THE AGENCY:

1. Review this guideline and communicate the information contained in it to all staff.
2. Review all related agency policies and procedures for compliance with this guideline.
3. Incorporate any new requirements into existing and new policies and procedures, as required.
4. Ensure that a SMIS Access Manager and Alternate has been designated for your site, that all staff are aware of their role and responsibilities and that their contact information has been submitted to smishelp@toronto.ca from the e-mail box of the Executive Director of your agency**. Please note that this information must be submitted within one month of the execution of the 2010 Operating Agreement with the City.**
5. Ensure each SMIS user has been trained and received a copy of the SMIS Privacy Guideline.
6. Ensure that the SMIS Bed Log is printed, completed and signed at each final bed count and kept on file at the site.
7. Continue to use and submit the Weekly Occupancy Form to Hostel Services until September 1, 2010.

If you have any questions about Hostel Services Guideline 2009-34, please call your Agency Review Officer.

Trish Horrigan
Manager, Operations & Support Services
Hostel Services
Shelter, Support & Housing Administration Division

APPENDIX 1

Shelter Management Information System
User Responsibility and Confidentiality Agreement

User Name: (print) _____

Shelter Name: _____

User Email Address: _____

This agreement is between the Shelter/Agency (Employer) and the staff person (Employee/User) who will use the City of Toronto's Shelter Management Information System, called SMIS.

Your User ID and password give you access to SMIS. You are required to use your User ID and password in accordance with the responsibilities set out below. You understand that failure to adhere to the following responsibilities may result, at the City of Toronto's sole discretion, in revocation of your User ID, password and access to SMIS.

You are asked to initial each item below to indicate that you understand and accept the terms and conditions for the use of your User ID, password and access to SMIS.

_____ I understand and agree that I am given access to SMIS for the sole purpose of providing services to clients in the shelter at which I am employed.

_____ I understand and agree that activities carried out using SMIS are logged and subject to audit by the City of Toronto system administrator upon request by a manager at my shelter or another authorized person.

_____ I understand and agree that my User ID and password are for my use only and I will not share these with anyone.

_____ I will take all reasonable steps to keep my password physically secure and to prevent its disclosure, modification, and use by any other person.

_____ I will be responsible for all inputs/changes/modification/deletions entered in the system under my User ID and password.

_____ I will not permit anyone to view information in the SMIS system except for authorized Users as determined by my employer and the clients to whom the information pertains.

_____ I will only view, obtain, disclose or use the database information that is necessary to perform my job.

_____ I **will log off** SMIS whenever I leave the work area where the computer is located to minimize the possibility of a breach in client confidentiality and system security.

_____ I shall not leave unattended a computer that has SMIS "open and running".

_____ If I work at more than one shelter, I shall access only the files for clients in the shelter at which I am working, while at that shelter.

_____ I shall keep hard copies of client information printed from SMIS in a secure file.

_____ When hard copies of client information from SMIS are no longer needed, I shall ensure that they are properly destroyed or archived in a manner that maintains their confidentiality.

_____ If I notice or suspect a security breach, I will immediately notify my supervisor or manager in my shelter. I shall also notify my supervisor or manager immediately if there is a possibility that my password may have been compromised in any way.

I understand and agree to comply with all the statements listed above. I also acknowledge and agree that:

- I will be allowed access to confidential information and/or records in order that I may perform my specific job duties.
- I will not disclose confidential information and/or records except in accordance with the staff code of conduct and confidentiality policy for my workplace.
- I will treat clients and partner agencies with respect, fairness and good faith, and will maintain high standards of professional conduct in my capacity as a SMIS User.

This agreement is valid for the duration of my employment at this shelter / agency.

_____

User Signature Date

Shelter/Agency Executive Director or Designate:

_____ _____ _____

Name (please print) Signature Date

APPENDIX 2

Privacy Breach Protocol

Background

SMIS users are collecting and utilizing information to which the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) applies. As such, it is a legal requirement under section 3 of Ontario Regulation R.R.O. 1990, Reg. 823 that all information to which MFIPPA applies is safeguarded against inappropriate and/or negligent disclosure.

Personal information is recorded information about an identifiable individual.

This 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 the Agency, any System User, any Agency Staff, or any other persons employed, or contracted to perform work, by the Agency, intentionally or unintentionally, discloses personal information or records containing personal information contrary to the requirements of this Agreement, MFIPPA, or any other relevant agreement and/or legislation (a "Privacy Breach"). Examples of Privacy Breaches include instances where a computer or peripheral device is lost or stolen or sensitive information is mailed to an incorrect 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.

Protocol

When a Privacy Breach involving the SMIS is discovered, Agency Staff and System Users must immediately undertake the following protocol (the "Protocol"):

Step 1: Confirm

The relevant Agency Staff and the Access Manager shall confirm that a Privacy Breach has occurred.

If the relevant Agency Staff determines that a Privacy Breach has taken place, that Agency Staff shall ensure that the Access Manager is immediately informed of the breach.

The Access Manager will immediately evaluate the Agency Staff's determination that a Privacy Breach has occurred.

Step 2: Contact

Where a Privacy Breach has occurred, the Access Manager shall immediately, and within no more than 24 hours of discovery of the Privacy Breach, establish contact with the individual at the City identified in section 3.8 of this Schedule (the "City Contact").

The Access Manager, upon notification to the City Contact, shall follow all instructions of that individual, in relation to the alleged Privacy Breach.

Without limiting the aforementioned, after notifying the City Contact, the Access Manager shall immediately, and within no more than 24 hours of discovery of the Privacy Breach, notify all persons required and/or requested by the City Contact.

The Access Manager shall ensure that no persons other than those required by the City or the City Contact are informed of the breach, except where otherwise required by law.

Step 3: Contain and Cooperate

In the event of a Privacy Breach or an alleged Privacy breach, the Access Manager shall comply with all requests of the City Contact in relation to any such actual or alleged Privacy Breach, including, but not limited, any requirements to:

(a) suspend any practice that may have caused or contributed to the Privacy Breach until instructed otherwise by the City Contact;

(b) notify, where applicable, any required law enforcement officers of the actual or alleged Privacy Breach;

(c) undertake reviews of policies and practices which may have caused or contributed to the actual or alleged Privacy Breach; and

(d) retrieve any documentation that has been disclosed inappropriately or pursuant to a Privacy Breach.

(e) provide any information to the City and the City Contact related to any policies or procedures that may have caused the actual or alleged Privacy Breach

(f) complete all documentation required or requested by the City in relation to the Privacy Breach or any documents related thereto.

Step 4: Document

The Access Manager shall ensure that the Privacy Breach Information Summary, attached hereto as Appendix 3 is fully completed within 24 hours of discovery of the Privacy Breach. Without limiting the aforementioned, the Access Manager shall ensure compliance with all other requirements related to the Privacy Breach Information Summary.

Step 5: Mitigation

In the event of a Privacy Breach or an alleged privacy breach, the Access Manager shall comply with all requests of the City Contact in relation to any such actual or alleged Privacy Breach, including, but not limited, any requirements to:

(a) educate or train, or re-educate or re-train, Agency Staff, as required;

(b) provide notices, letters, or correspondence to required individuals affected by the Privacy Breach

(c) alter or adjust pre-existing policies

(d) retrieve the record or information that is the subject of the Privacy Breach, where possible

(e) comply with all other reasonable requests of the City Contact in relation to the Privacy Breach

APPENDIX 3

Privacy Breach Information Summary

Date of Privacy Breach:

Date Reported to SMIS Privacy Contact:

SMIS Privacy Contact Name:

Agency Staff Name:

SMIS Access Manager Name:

Position Title:

Address:

Telephone Number:

Email address:

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

Was a third-party involved, and if so, please describe any such involvement?

Summary of Issue and Action Taken:

Investigation details

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

Consultation with SMIS Privacy Contact

Representative Future Action/Follow Up:

APPENDIX 4

NOTICE OF COLLECTION

Your personal information is collected under the legal authority of the City of Toronto Act, 2006, 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, Shelter, Support and Housing Administration Division, Telephone no. 416-392-8741, Metro Hall, 55 John St. 6th Floor, Toronto, Ontario M5V 3C6.

Statement to be read to client when collecting information by telephone:

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.

APPENDIX 5

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 and 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 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 and the request is time sensitive 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.(develop a template letter)
- 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 are to 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 heath 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) ***Schedule 2***.

    - 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 those 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 completed 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 are 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 416-392-9684. Any questions related to these guidelines can be directed to the SMIS Privacy Contact at 416-392-8741.

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

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 #: