SAFER OTTAWA NEIGHBOURHOODS: A MULTI-STAKEHOLDER APPROACH TO PROBLEM ADDRESSES – PRIVACY PROCEDURES

1.1 FRAMEWORK PRIVACY PROCEDURES

The **Multi-Stakeholder Framework for Safer Communities and Neighbourhoods (Framework)** procedures are the foundation that clearly states the underlying beliefs and guides the actions of the safety and service partners. The procedures ensure that the Framework:

- carefully targets its legal mandate of providing public safety;
- appropriately tailors the powers to intervene and act;
- properly balances public safety with the established rights and freedoms; and
- ensures proper handling and treatment of personal information.

The Framework Privacy Procedures are intended to provide the safety and service partners with guidance on the appropriate sharing and protection of personal information for the purposes of responding to and resolving public safety issues from repetitive sites of continual danger and threatening activities in a coordinated manner through the NAST.

The Framework Privacy Procedures are based on the Canadian Standard Association (CSA) Model Code for the Protection of Personal Information, which became recognized as a national standard for privacy protection in 1996, is used across Canada and the world as the basis for privacy legislation, policies and procedures and includes the following ten principles: accountability, identifying purposes, consent, limiting collection, limiting use, disclosure and retention, accuracy, safeguards, openness, individual access, and challenging compliance. The Privacy Procedures also draw on:

- consultation with OPS, OCH security and legal team, health practitioners with Community Health and Resource Centres, and City of Ottawa by-law and legal teams;
- a meeting of the Inter-Agency Information Sharing Working Group (IAISWG), which provided insight into similar work currently underway in Saskatchewan and Ontario, other cross-sector sharing protocols, and relevant privacy legislation, as well as various documents provided by IASWG related to legislative interpretation on information sharing; and
- the Saskatchewan Information Sharing Issues Working Group, Interim Information Sharing Guidelines for Community Mobilization and Hubs, April 2013, and the Memorandum of Understanding between the Executive Steering Committee of CMPA Respecting Community Mobilization: Prince Albert (CMPA).

PRIVACY PRINCIPLE #1: ACCOUNTABILITY

The NAST will appoint a NAST Lead who has responsibility for ensuring adherence to the Framework and these privacy principles, and for ensuring follow up on action items. Other safety and service partners may be appointed as the Privacy Leads for other NASTs, based on the problem address under discussion. The NAST Lead will:

- confirm that information sharing within the NAST aligns with these procedures;
- direct access to information requests and privacy complaints to the relevant parties; and
- promote good practice with respect to privacy.

Each service and safety partner is responsible for collecting, using, disclosing, and protecting personal information involved in the NAST in accordance with the applicable legislation (described below).

Name of Partner	Applicable Privacy Legislation
Ottawa Police Service (OPS)	Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) Police Services Act
City of Ottawa – Emergency and Protective Services	MFIPPA
Ottawa Community Housing (OCH)	MFIPPA Housing Services Act, 2011 Residential Tenancies Act
Children's Aid Society of Ottawa (CASOTT)	Personal Health Information Protection Act, 2004 (PHIPA) Ontario Child and Family Services Act
Community Health and Resource Centres (CHRCs)	PHIPA

Each partner is also responsible for ensuring that individuals the partner assigns to the NAST:

- understand their accountability to protect personal information shared within the NAST;
- understand whether they are properly collecting, using, and/or disclosing personal information in accordance with relevant privacy legislation;
- have executed a confidentiality agreement;
- know how to detect and report privacy issues; and
- have undergone privacy training.

Only partners with privacy programs that outline the appropriate collection, use, disclosure, retention, and protection of personal information shall be included in the NAST in order to ensure continuity of the protection of personal information once partners return to their organizations. Privacy Officers at the partner organizations

continue to be responsible for the appropriate management of personal information by individuals within their respective organizations.

PRIVACY PRINCIPLE #2: IDENTIFYING PURPOSES

Safety and service partners must only share personal information at the NAST for the purposes of responding to and resolving public safety issues from repetitive sites of continual danger and threatening activities in a coordinated manner.

PRIVACY PRINCIPLE #3: CONSENT

Safety and service partners should be aware of the consent requirements of relevant legislation (e.g. Police Services Act) and ensure they have the proper authority to collect personal information at the outset. Under MFIPPA, safety and service partners may rely on consent to use or disclose personal information if the person to whom the information relates has identified that information in particular and consented to its disclosure (and the party receiving the information has the legal authority to collect it). Under PHIPA, safety and service partners who are also health information custodians may disclose personal health information about an individual without consent in certain situations:

- To eliminate or reduce a significant risk of serious bodily harm to a person or a group of person(s) (s. 40(1));
- To the Public Guardian and Trustee, the Children's Lawyer or a Children's Aid Society (s. 43(1)(e)); and
- To a person carrying out an inspection or investigation under a warrant, or provincial or federal law.

Under the Police Services Act, the Police Chief, or a person designated by him or her, may disclose personal information in certain situations for the:

- Protection of the public
- Protection of victims of crime (PSA Part IV, s41(1.2)

The safety and service partners will rely on informed consent from the individual involved in the problem address or their parents/guardians, where appropriate and where they have proper authority to do so under MFIPPA or other legislation. Informed consent will be the preferred method of enabling the sharing of information among safety and service partners and should be sought wherever possible. Informed consent will allow the individual to understand and agree to:

- What personal information or personal health information will be shared;
- With whom;
- For what purpose; and
- For how long (consent can be withdrawn at any time).

NAST members should discuss with their Privacy Officers whether consent may be relied on to share personal information at the NAST.

PRIVACY PRINCIPLE #4: LIMITING COLLECTION

The safety and service partners will ensure they have the proper authority to collect personal information. Once the personal information is lawfully collected, the safety and service partners will only share necessary and relevant information about each problem address required to generate an effective and sustainable solution. To this end, each safety and service partner will review the information that the partner intends to share (and other partners will collect) at the NAST and determine what information should be de-identified or limited to protect the privacy of individuals involved in the problem address (e.g. sharing that the tenant is seeking addiction treatment, but not the specifics of this treatment) prior to sharing it at the NAST. In this review, the partner will ensure that personal information is shared only for the following purposes:

- to understand the information about each problem address more comprehensively and accurately;
- to suitably tailor the interventions for each problem address; and
- to target effective interventions at each of the problem addresses.

PRIVACY PRINCIPLE #5: LIMITING USE, DISCLOSURE, AND RETENTION

Limiting use and disclosure

Each safety and service partner will:

- only collect, use, and disclose personal information in accordance with their responsibilities under relevant privacy legislation and on a "need to know" basis;
- not record personal information discussed in the NAST, except recording action items that the partner will carry out to respond to and resolve the problem address issues and only to the extent they are involved in addressing acutely elevated risk factors;
- conduct discussions in the NAST only on issues of elevated risk;
- conduct discussions in the NAST in a manner that uses de-identified information to the greatest extent possible;
- limit the sharing of identifiable information to that which is necessary to discuss a problem address;
- ensure that the single point of contact at the NAST complete proper screening and privacy training prior to introduction to the NAST and a problem address (see Accountability above); and
- obtain informed consent of the client whenever possible (see Consent above).

Disclosure of personal information pertaining to a specific problem address can only be communicated at the NAST among the appointed individuals of the safety and service partners. The safety and service partners will keep this information in the strictest confidence and not communicate it to any other person.

Limiting retention

The safety and service partners will be attentive to any form of record keeping and note-taking that could lead to potential privacy issues by only recording de-identified action items, where possible, and follow up notes. Each safety and service partner will each retain his or her own information and no central repository of information will be retained by the NAST.

Partners will make reasonable efforts to ensure their individual notes are adequately protected and not left in public places (e.g. briefcase, trunk of car, office in plain view). Personal information collected by the safety and service partners will be subject to retention periods that apply to that organization.

Once the personal information is no longer required, the NAST Lead and the safety and service partners will securely erase media or shred hardcopies so that the reconstruction of the record is not possible.

All information releases to the media or public will be approved by the core safety and service partners, who will also assign a spokesperson from one of the partner organizations.

PRIVACY PRINCIPLE #6: ACCURACY

Accuracy of information is important to targeting and tailoring interventions to respond to a problem address, often involving complexities with numerous responsible parties. The safety and service partners need accurate information to minimize the possibility of ineffective and/or inappropriate interventions.

To this end, it is the responsibility of the safety and service partners to share accurate, complete, and up-to-date personal information as it relates to the specific problem address. If there are risks that the personal information may not be accurate, such risks should be stated alongside the personal information being shared.

PRIVACY PRINCIPLE #7: SAFEGUARDS

The NAST will implement administrative, technical, and physical safeguards to protect personal information from inappropriate collection, use, and disclosure.

Administrative

The NAST will have the following administrative safeguards in place:

- Confidentiality/non-disclosure agreements signed by NAST members; and
- Privacy training to be completed by NAST members.

A privacy breach is the inappropriate collection, use, or disclosure of personal information. In the event of a privacy breach of personal information shared at the NAST, the following steps will be immediately taken by the safety and service

partners to resolve the breach: containment, notification, and remediation. The NAST Lead will confirm that a breach occurred and coordinate the breach management activities as described below. The partner who is most responsible for the privacy breach will lead breach resolution activities.

Technical

Safety and service partners are responsible and compelled to be diligent in ensuring that any of their records arising out of NAST meetings are:

- kept separate from other business/work files in a dedicated and secure storage device or encrypted and password protected if the file is electronic;
- stored securely in their workplaces and are not in plain view when not in use; and
- not left in places where there may be opportunities for privacy breaches, such as vehicles and briefcases.

Physical

In addition to the physical security measures listed under "Limiting Retention" above, the NAST Lead will ensure that physical safeguards are in place during NAST meetings. For example, NAST meetings will be held in a secure, private location.

PRIVACY PRINCIPLE #8: OPENNESS

Safety and service partners are committed to openness and transparency. Therefore, Crime Prevention Ottawa will also make publically-available on its website information about the Framework.

The Notice of Collection posted by each institution will include a description of the collection, use, and disclosure of personal information for the purposes of responding and resolving a problem address.

PRIVACY PRINCIPLE #9: ACCESS AND CORRECTION

MFIPPA and PHIPA both include a right for individuals to access information, subject to certain exceptions.

The NAST Lead will direct any request for access to, or correction of, personal information to the relevant safety and service partner. The safety and service partners will address access and correction of information.

PRIVACY PRINCIPLE #10: CHALLENGING COMPLIANCE

NAST partners are committed to reviewing the Framework, including privacy procedures, on a periodic basis.

The NAST members will direct any complaints to the relevant safety and service partner.