

# ONPHA Sample Policies: Video Surveillance Systems

Revised July 2009

---



The following sample policy was developed by ONPHA in response to feedback received from the membership surrounding the use of video surveillance systems. Some members reported that, while they have implemented video surveillance systems at various properties within their portfolio, they have not developed policies and procedures to govern their use and the protection of the personal information collected.

It is extremely important that all providers who have installed a video surveillance system have a policy in place governing its use and the responsibilities of the organization. Housing providers that are considering the installation of such a system should review this sample policy to ensure that they fully understand the obligations that accompany the installation and use of this technology.

ONPHA's Video Surveillance Systems sample policy is a general policy which must be customized to meet the unique circumstances of your organization. Once the sample policy has been modified to meet your needs, it is recommended that you review the changes with a legal professional to ensure that the changes are consistent with the appropriate legislation and that the non-profit remains protected.

Highlights from the ONPHA sample policy include:

- staff training requirements, including identifying the individual(s) responsible for monitoring and maintaining the system and their unique responsibilities and obligations;
- the conditions under which it is appropriate to install a video surveillance system and how it should be installed and positioned;
- the treatment, including the collection, release, and destruction of the personal information gathered via this technology; and,
- the notification requirements for tenants, staff, service providers, and staff.

This sample policy also contains sample signs and forms that providers can modify, including:

- a sample sign to inform tenants and visitors of the video surveillance being used on-site;
- a sample Release of Information form and template log to document the destruction of video surveillance records; and,
- a sample clause that should be included in all of your agreements with third party service providers.

Remember, that while a housing provider may install video surveillance technology for legitimate operational purposes, such technology does infringe upon the privacy of your tenants, their guests, service providers, and housing provider staff. It is therefore extremely important to ensure that your organization is operating in accordance with all relevant privacy legislation.

**The following sample policy must be customized so that it meets the unique needs and context of your organization. Please review the sample policy and reflect on what elements of the sample policy are appropriate for your organization and what must be changed or removed so that it meets your needs.**

**If you have any questions or comments about this sample policy, please contact ONPHA's Management Support department by email (<mailto:management.help@onpha.org>) or by telephone (1-800- 297-6660).**

## **POLICY TITLE: Corporate Policy - Video Surveillance Systems**

### **Policy Statement**

#### **1. Purpose**

- (a) It is the policy of [INSERT NAME OF YOUR NON-PROFIT] to utilize video surveillance as necessary in accordance with this Corporate Policy - Video Surveillance Systems (the "Policy").
- (b) Video security surveillance systems are a resource used by the [INSERT NAME OF YOUR NON-PROFIT] at selected sites within the management jurisdiction of [INSERT NAME OF YOUR NON-PROFIT] for the purpose of increasing the safety and security of tenants, staff and members of the public, to protect public safety, our corporate assets and property and to detect and deter criminal activity and vandalism.
- (c) [INSERT NAME OF YOUR NON-PROFIT] is authorized to conduct video surveillance under Section 28(2) of the *Municipal Freedom of Information and Protection of Privacy Act* (MFOIPPA) or Section 38(2) of the *Freedom of Information and Protection of Privacy Act* (FOIPPA), as applicable. The [INSERT NAME OF YOUR NON-PROFIT] recognizes that video surveillance technology has the potential for infringing upon an individual's right to privacy and although video surveillance technology may be required for legitimate operational purposes, its use must be in accordance with the provisions of MFOIPPA or FOIPPA, as applicable, and any other applicable privacy laws.
- (d) This Policy does not require or guarantee that a camera or recording equipment will be recording or monitored in real time at all times.

**[Note to Housing Provider: Please note that this Policy does not permit the use of covert surveillance.]**

- (e) All **[INSERT NAME OF YOUR NON-PROFIT]** employees involved in the operation of this video surveillance program have been trained on this Policy and their statutory obligations in performing their duties and functions related to the operation of the video surveillance system and **[INSERT NAME OF YOUR NON-PROFIT]**'s video surveillance program.
- (f) **[INSERT NAME OF YOUR NON-PROFIT]** employees may be subject to discipline if they breach this Policy or applicable privacy laws.

## **2. Collection, Use and Disclosure**

“Personal Information” as collected by **[INSERT NAME OF YOUR NON-PROFIT]** pursuant to this Policy means recorded information about an identifiable individual, including, but not limited to, information relating to an individual’s race, colour, national or ethnic origin, sex, age. If a video surveillance system displays such characteristics of an identifiable individual or the activities in which he or she is engaged, its contents will be considered “personal information”.

- (a) Personal Information collected by **[INSERT NAME OF YOUR NON-PROFIT]** pursuant to this Policy will be recorded and will only be used for the purposes set out herein, or as may otherwise be permitted or required by law. For example, Personal Information may be disclosed to the police or other law enforcement agencies in Canada to aid an investigation. In the event of a reported or observed incident, the review of recorded information may be used to assist in the investigation of the incident.
- (b) Disclosure of storage devices should be made to authorities only upon the presentation by the authorities of a warrant or court order for the same and upon completion of a form setting out the name of the individual(s) who took the storage device, under what legal authority, the date and whether the storage device will be returned or destroyed after its use by the authorities.
- (c) Storage devices containing Personal Information may be shared with third party service providers who have a need to access such information and only upon them entering into an agreement to keep such information confidential and handling the Personal Information in accordance with the terms of this Policy and applicable law.

### **3. Protecting your Personal Information**

- (a) Personal Information collected by [INSERT NAME OF YOUR NON-PROFIT] is protected to avoid unauthorized access. Access to the storage devices where recorded Personal Information is retained is only permitted by personnel authorized in accordance with this Policy. Systems are password protected.

### **4. Access**

The Personal Information recorded by video surveillance is subject to freedom of information and privacy laws. You have the right to access the Personal Information we hold relating to you, including on video recordings. You may request access by contacting [title] at [contact information.]. Requests for Access may be denied in certain circumstances as set out in MFOIPPA and FOIPPA, including where disclosure would interfere with a law enforcement matter or investigation or unjustifiably invade another person's privacy. **[Note to Housing Providers: When disclosing recordings to individuals who are in them, you must not show information about any other identifiable individuals. This could be done through using technology to hide identity on the video.]**

### **5. Retention**

- (a) Personal Information will only be retained as long as necessary to fulfill the purposes for which it was collected pursuant to this Policy, or as otherwise permitted or required by law.
- (b) Personal Information that has not been viewed for law enforcement or public safety purposes should be erased no more than 72 hours after recording. Personal that has been viewed for law enforcement and public safety purposes must be retained for a certain period thereafter (the requirement is one year in accordance with Section 5 of Ontario Regulation 823 under MFOIPPA unless a shorter retention period is specified by law).

### **6. Disposal**

Old storage devices will be securely disposed of in a way that the personal information cannot be reconstructed or retrieved. They may include shredding, burning or magnetically erasing the personal information. Disposal of records will be recorded in writing.

## **7. Breach**

In the event of a collection, use, disclosure or retention in violation of applicable privacy laws, [INSERT NAME OF YOUR NON-PROFIT] will comply with all recommendations of the Office of the Information and Privacy Commissioner of Ontario in responding to breaches. The General Manager will respond to any inadvertent disclosures of Personal Information. Any breach of the Acts will be reported to the Board of Directors.

## **8. Training**

- (a) This policy and any related processes or guidelines must be incorporated into training and orientation programs of [INSERT NAME OF YOUR NON-PROFIT]. Training programs addressing staff obligations under the relevant legislation shall be conducted as necessary.
- (b) [INSERT NAME OF YOUR NON-PROFIT] staff and service providers are required to review and comply with this Policy and applicable privacy laws in performing their obligations related to the video surveillance system.
- (c) [INSERT NAME OF YOUR NON-PROFIT] staff that violates this Policy or applicable privacy laws may be subject to discipline.

## **9. Designated Responsibilities**

- (a) [INSERT NAME OF YOUR NON-PROFIT] will maintain control of and responsibility for the video surveillance system on its premises at all times.
- (b) The [INSERT NAME OF YOUR NON-PROFIT] General Manager is responsible for [INSERT NAME OF YOUR NON-PROFIT]'s compliance with applicable privacy laws and this Policy.
- (c) The [INSERT NAME OF YOUR NON-PROFIT] Manager of Technical Services is responsible for ensuring the establishment of procedures for video surveillance equipment, in accordance with this Policy and any legal requirements.
- (d) The [INSERT NAME OF YOUR NON-PROFIT] Manager of Technical Services is further responsible for the life-cycle management of authorized video security surveillance systems, specifications, equipment standards, installation, maintenance, replacement, disposal and related requirements (e.g. signage), including:

- (i) Documenting the reason for implementation of a video surveillance system at the designated area.
- (ii) Maintaining a policy regarding the locations of the reception equipment.
- (iii) Maintaining a list of personnel who are authorized to operate the systems and access any recordings, including the circumstances under which access is permitted. Logs must be kept of any access to such recordings.
- (iv) Maintaining a record of the times when video surveillance will be in effect.
- (v) Assigning a person responsible for the day-to-day operation of the system in accordance with policies, procedures and direction/guidance that may be issued from time-to-time.

## **10. Installation and Placement**

When using video surveillance equipment, [INSERT NAME OF YOUR NON-PROFIT] will comply with the following:

- (a) The use of each video surveillance camera should be justified on the basis of verifiable, specific reports of incidents of crime or significant safety concerns or for crime prevention. Video cameras should only be installed in identified public areas where video surveillance is a necessary to protect public safety, corporate assets and property, including detecting and deterring criminal activity and vandalism.
- (b) Privacy intrusion should be minimized to that which is absolutely necessary to achieve [INSERT NAME OF YOUR NON-PROFIT]'s required, lawful goals.
- (c) Equipment to monitor video surveillance will be installed in a strictly controlled access area. Only personnel authorized under this Policy may access to the access area and the equipment. Monitors showing personal information captured by the video surveillance equipment will not be located in a way that that enables the public to view it.
- (d) Equipment will be installed in such a way that it only monitors those spaces that have been identified as requiring video surveillance. Video surveillance

equipment will never monitor the inside of areas where the public or employees have a higher expectation of privacy such as change rooms and washrooms. Equipment should not be focused on individuals' doors or through windows or through windows of neighbouring buildings.

- (e) Adjustment of the camera position will be restricted, if possible, to ensure only designated areas are being monitored.

## **11. Service Providers**

- (a) [INSERT NAME OF YOUR NON-PROFIT] will ensure that any agreements between [INSERT NAME OF YOUR NON-PROFIT] and its service providers state that records under the video surveillance program remain under [INSERT NAME OF YOUR NON-PROFIT]'s control and subject to applicable privacy laws.
- (b) Violation of this Policy or applicable privacy laws by service providers will be considered a breach of the contract.
- (c) Agreements with Service Providers should ensure that employees of service providers sign written confidentiality agreements, including complying with this Policy and applicable privacy laws in respect of personal information collected under the video surveillance program.

## **12. Audit of Surveillance Policy and Practices**

- (a) [INSERT NAME OF YOUR NON-PROFIT] will ensure that the use and security of its video surveillance program and equipment is subject to regular audits, at least once a year, to address compliance with this policy and applicable laws. The audit will also include a review of whether ongoing video surveillance is justified based on the requirements set out in this policy. Any deficiencies or concerns identified by the audit will be addressed immediately.
- (b) [INSERT NAME OF YOUR NON-PROFIT] staff and service providers will be made aware that their activities are subject to the audit and that they may be called upon to justify their surveillance.
- (c) Any questions or concerns related to [INSERT NAME OF YOUR NON-PROFIT]'s handling of personal information collected through video surveillance can be directed to:



[title]  
[address]  
[telephone]

### **13. Notification**

The public must be notified of the existence of video surveillance equipment by clearly written signs prominently displayed at the entrances, exterior walls, and interior of buildings and/or perimeter of the video surveillance areas. Signage must inform individuals of the legal authority for the collection of personal information; the principal purpose(s) for which the personal information is intended to be used and the title, business address and telephone number of the appropriate contact (Privacy Officer) at **[INSERT NAME OF YOUR NON-PROFIT]** in order to answer questions about its personal information management practices. A sample notification follows.

# **ATTENTION**



## **This Area May Be Monitored By Video Surveillance Cameras (CCTV)**

The personal information collected by the use of CCTV at this site is collected under the authority of the *Municipal Freedom of Information and Protection of Privacy Act* or the *Freedom of Information and Protection of Privacy Act*, as applicable. This information is used for the purposes of promoting public safety and reducing crime at this site.

**Any persons who tamper with or  
destroy video surveillance equipment  
will be subject to criminal proceedings.**

Any questions about this collection can be directed to: Property Manager, La Coopérative d'habitation Beuparlant Inc. at (905-735-8376), (52 promenade Richelieu, Welland, Ontario)

(e-mail – [louised@nphcr.ca](mailto:louised@nphcr.ca)).



## **APPENDIX B: RELEASE OF PERSONAL INFORMATION / VIDEO SURVEILLANCE**

*[The following form should be completed any time that staff receive a request from municipal or provincial police services or other third parties to release or view information gathered through video surveillance conducted by the non-profit.]*

Date:		Name of Staff:	
-------	--	----------------	--

### **SECTION A: Information from individual(s) requesting information**

Name:		Organization:	
Address:			
Telephone:		Email:	

Is this information being requested as part of an on-going police investigation? ☐ Yes ☐ No

If no, why is this information being requested?

Has a warrant or court order been produced authorizing the individual(s) to view or remove the information requested? ☐ Yes ☐ No

### **SECTION B: Description of information sought**

(include information such as date, time, camera number, individual(s) of interest, and a description of the incident)

---

---

---

---

---

---

---

---

Will the information removed be returned to the organization or destroyed? ☐ Returned ☐ Destroyed

The information taken will be transported, stored, and, if necessary, destroyed in accordance with all relevant provincial and federal laws governing the use of Personal Information.

---

Signature

---

Date

---

Name (*please print*)

## **APPENDIX C: RECORD KEEPING LOG: DESTRUCTION OF VIDEO SURVEILLANCE**

*[The following form should be completed any time that staff destroy information gathered through video surveillance conducted by the non-profit.]*

<b>Date</b>	<b>Name of Staff Person</b>	<b>Tape or File Identification Number</b>	<b>Destruction Method</b>



## **APPENDIX D: SAMPLE CONTRACT CLAUSES**

**The following sample clause can be inserted into contracts or agreements with third party service providers.**

While on [INSERT NAME OF YOUR NON-PROFIT] property visitors, guests, and service providers may be recorded by video surveillance equipment installed throughout the premise. The Personal Information recorded by such equipment is the property of [INSERT NAME OF YOUR NON-PROFIT] and will be collected, stored, and destroyed in accordance with all appropriate provincial and federal laws and in accordance with the non-profit's *Video Surveillance Systems Policy* (Policy number: [POLICY NUMBER]).