OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

OIPC GUIDELINES FOR THE USE OF

VIDEO SURVEILLANCE SYSTEMS IN SCHOOLS

February 13, 2013

TABLE OF CONTENTS

Acknowledgement

The following *Guidelines for the Usage of CCTV Systems in Schools in Newfoundland and Labrador* were prepared following consultation with the Department of Education, all five school districts, the NLTA and the Newfoundland and Labrador Federation of School Councils. Furthermore, a cross jurisdictional study of best practices in other provinces and territories in Canada was conducted for advice and guidance. The OIPC gratefully acknowledges the assistance provided by all the participants in this consultative process, and especially the Ontario Office of the Information and Privacy Commissioner whose *Guidelines for Using Video Surveillance Cameras in Schools* were a source of guidance and inspiration.

Introduction

Closed circuit television cameras (CCTV) have been in common usage for approximately the past two decades, but their first known usage was over 70 years ago. It has become quite common in Europe and North America to see CCTV in stores, airports and banks, and it is becoming increasingly more likely for CCTV to be found in government buildings, on streets and even in schools. While it is not known precisely when the first CCTV system was installed in a school it is estimated that this occurred in the mid 1990s.

There are approximately 269 K to 12 schools in Newfoundland and Labrador. Over 25% or roughly 70 schools are currently using CCTV systems. Additionally, there are CCTV systems in place on 34 school buses in this province. The Office of the Information and Privacy Commissioner (OIPC) is concerned about the proliferation of video surveillance from a privacy perspective. We hope to ensure that CCTV systems, whether installed or planned, are only utilized to the extent that they are necessary to address real and serious problems.

More often than not, when asked why CCTV systems are in place or are being put in place the response is either to protect students from violence or to prevent vandalism to schools. While no one can argue with the goals identified, it is essential that schools and school districts start from a position of recognizing that privacy is a right. We must also start with the recognition that there is a law in place (the *Access to Information and Protection of Privacy Act*), which places limits on what is appropriate in the application of CCTV by school districts in the province. Furthermore, it is crucial that schools and school districts in this province have a comprehensive set of guidelines to follow when utilizing CCTV systems.

CCTV systems are not a cure-all. CCTV should only be used as a last resort where the school can justify its use on the basis of verifiable, specific reports of incidents of theft, violence, breaches of security, public safety concerns or other compelling circumstances. Options for other less privacy-invasive means of deterring or detecting crime or inappropriate activity or enhancing public safety must be explored before video surveillance is entertained as a solution. It is also a good idea to consult affected individuals (including students, parents, and staff) for their views before making a final decision.

The Office of the Information and Privacy Commissioner is an independent Office of the House Assembly. The Commissioner has a broad range of responsibilities and powers under the *Access to Information and Protection of Privacy Act (ATIPPA)*. Along with oversight powers to conduct reviews of decisions and investigate privacy breaches, the Commissioner can make recommendations to public bodies in order to uphold the *ATIPPA* and to encourage compliance with the *ATIPPA*. The Commissioner can also comment on privacy issues through the news media or by reporting on privacy issues in his Annual Report to the House of Assembly.

The OIPC has developed these *Guidelines* to assist school districts and individual schools to develop policies and procedures to comply with the *ATIPPA* while utilizing CCTV systems. The *Guidelines* should also be utilized by any school or school district which is undertaking an assessment as to whether or not CCTV is an appropriate solution to problems being experienced. These *Guidelines* stress the need for privacy compliant measures to be established and privacy-first policies to be developed prior to the installation of CCTV systems. It is the recommendation of the OIPC that all schools currently utilizing CCTV systems re-evaluate their programs to ensure compliance with *ATIPPA* and these *Guidelines*, and furthermore, that any school or school district contemplating additional installation of CCTV systems do so only in harmony with these *Guidelines* and in full compliance with *ATIPPA*.

Applicability of Guidelines

These *Guidelines* have been developed to apply to situations where permanent CCTV systems have been placed or are intended to be placed on school property. These *Guidelines* are not intended to deal with instances where school officials videotape a specific event (such as a school play, concert or graduation ceremony), or an isolated instance where a classroom is videotaped for educational or research purposes (for example, where a student teacher is required to record his or her lesson as part of an assignment for a work placement).

These *Guidelines* do not apply to covert surveillance, or surveillance when used as a case-specific investigation tool for law enforcement purposes where there is statutory authority and/or the authority of a search warrant to conduct the surveillance.

However, the *Guidelines* will apply in any instances where a school district has set up permanent or semi-permanent cameras to monitor students, including instances where cameras are used in school buses. Where school districts have entered into agreements with service providers to provide bussing, districts should take steps to ensure that the practices of service providers also adhere to the *Guidelines*. This requirement is dealt with at greater depth in these *Guidelines*.

ATIPPA

The *Access to Information and Protection of Privacy Act* was passed by the Newfoundland and Labrador House of Assembly in March of 2002. The access provisions were proclaimed into force on January 17, 2005 and the privacy provisions were proclaimed into force on January 16, 2008. The *ATIPPA* replaces the old *Freedom of Information Act* which came into effect in 1981. The *ATIPPA* governs access to records in the custody of or under the control of a public body and sets out requirements for the collection, use, and disclosure of personal information contained in the records they maintain.

A public body is defined in section 2 of the legislation and includes provincial departments and agencies, **school districts**, public post-secondary institutions, health boards and municipalities.

The protection of privacy provisions (Part IV) of the *ATIPPA* limit the extent and means by which public bodies can collect personal information, as well as the extent to which public bodies can use and disclose that information. Part IV also requires public bodies to make every reasonable effort to ensure that personal information is accurate and complete, to make reasonable security arrangements against unauthorized access, collection, use, disclosure or disposal of personal information, and to retain certain personal information about an individual in order to allow that individual a reasonable opportunity to obtain access to the information.

It is important to recognize that an individual has the right to file a complaint with the Information and Privacy Commissioner if that individual has reasonable grounds to believe that his or her personal information has been collected, used or disclosed by a public body in contravention of the provisions of Part IV of the *ATIPPA*. The school district, as a public body under *ATIPPA*, would

be the party required to respond to such a complaint. The Commissioner (or delegate) may investigate such a complaint, and if the complaint cannot be resolved informally, the Commissioner may make a finding as to whether or not the alleged collection, use or disclosure was in compliance with Part IV of the *ATIPPA*. Whether or not the Commissioner finds that the public body has complied with Part IV, the Commissioner may report the findings of his investigation in a published report and/or in the Commissioner's Annual Report to the House of Assembly. If the Commissioner finds that the public body has acted contrary to the provisions of Part IV, the Commissioner may also issue recommendations to ensure compliance with the *ATIPPA*.

Section 32 of the *ATIPPA* states:

> *32. No personal information may be collected by or for a public body unless*
>
> *(a) the collection of that information is expressly authorized by or under an Act;*
>
> *(b) that information is collected for the purposes of law enforcement; or*
>
> *(c) that information relates directly to and is necessary for an operating program or activity of the public body.*

Definitions

The following definitions are provided for assistance in interpreting these *Guidelines*:

- *Personal Information* as defined in the *ATIPPA* means recorded information about an identifiable individual, including

  (i) the individual's name, address or telephone number,

  (ii) the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,

  (iii) the individual's age, sex, sexual orientation, marital status or family status,

  (iv) an identifying number, symbol or other particular assigned to the individual,

  (v) the individual's fingerprints, blood type or inheritable characteristics,

  (vi) information about the individual's health care status or history, including a physical or mental disability,

  (vii) information about the individual's educational, financial, criminal or employment status or history,

  (viii) the opinions of a person about the individual, and

  (ix) the individual's personal views or opinions;

This definition provides a non-exhaustive list of examples of what constitutes personal information. **The requirement that personal information must be "recorded information about an identifiable individual" is critical. A recorded CCTV image of an identifiable individual meets this definition**.

- *Policy* refers to statements of the governing body's expectations defining the boundaries for governing body, administrative and staff action. Policies should reflect what is expected and be directed towards outcomes.

- *Procedures* are usually associated with each policy, detailing how something is done and the administrative action necessary to implement the policy.

- *Record*, as defined in Section 2 of the *ATIPPA*, means a record of information in any form, and includes information that is written, photographed, recorded or stored in any manner, but does not include a computer program or a mechanism that produced records on any storage medium.

- *Storage Device* refers to a videotape, computer disk or drive, CD-ROM, computer chip, or other device used to store the recorded data or visual, audio or other images captured by a video surveillance system.

- *CCTV* refers to any video surveillance systems or any video surveillance technology (including but not limited to video cameras; still frame cameras; digital cameras; and time-lapse cameras) that enables continuous or periodic recording (videotapes, photographs or digital images), viewing, or monitoring of public areas.

Collection of Personal Information Using CCTV Surveillance

Recording a person's image is a collection of personal information as defined by the *ATIPPA*. Prior to undertaking the installation of a CCTV surveillance system, school districts and schools should consider the privacy implications of such action. School districts and schools should conduct due diligence and training with respect to privacy awareness among staff and undertake a **Privacy Impact Assessment** prior to implementation.

Schools and school districts should draft policies and procedures that outline the roles and responsibilities of individuals or groups involved in the collection of personal information by CCTV.

Without limiting the content of these policies and procedures they should include:

- privacy-specific criteria that must be met before CCTV surveillance is undertaken including a description of alternative measures undertaken and their result;
- documentation of the decision, including a detailed rationale and purpose for the surveillance;
- written authorization at an appropriate level of the organization for undertaking video surveillance;
- limits on the collection of personal information to that which is necessary to achieve the stated purpose, including a description of the kind of information collected through the surveillance;
- limits on the use of the surveillance to its stated purpose and the duration of surveillance;
- details on the times when surveillance will be in effect and whether and when recording will occur;
- limits on the location and field of vision of the equipment including the rationale and purpose of the specific locations of equipment and fields of vision selected;
- limits on any special capabilities of the system, for example, sound, zoom, facial recognition or night-vision features;
- requirements that any recorded surveillance data or images be stored in a secure manner, including guidelines for managing video surveillance recordings, such as security, use, disclosure, and retention and appropriate details on the place where signals from the equipment will be received and monitored;
- designations of the persons in the organization authorized to operate the system, including the names of the individuals who may have viewed the surveillance and what the surveillance was used for;
- procedures for the masking of and/or removal of third party information;
- a retention period for the surveillance;
- procedures for the secure disposal of images including details on when and how images are to be disposed of;

- a service agreement with any third party hired to conduct the surveillance, if applicable;
- requirements that appropriate and ongoing training is provided to operators to make certain that they understand their obligations under all relevant legislation including *ATIPPA*, these Guidelines, and the organization's video surveillance policy;
- details on the process to follow if there is an unauthorized disclosure of images;
- procedures for individuals to access their own personal information captured through CCTV in compliance with the access provisions of the *ATIPPA*;
- sanctions for the organization's employees and contractors for failing to adhere to the policy; and
- the name and business contact information of the individual accountable for privacy compliance who can answer any questions or address concerns about the surveillance.

How to Decide Whether to Use a Video Surveillance System?

Prior to installing CCTV in schools or before deciding whether to expand or continue utilizing the CCTV systems already in place in your educational institution, the first and paramount consideration is as follows:

> ***Is there a real, pressing and substantial problem which is ongoing in nature that has not and cannot be mitigated by other less privacy intrusive measures?***

One incident, no matter how serious or severe, does not constitute a real, pressing and substantial problem. Nor does a series of minor incidents constitute a real, pressing and substantial problem. Schools must determine if there is a problem that requires the use of CCTV systems.

Specific, ongoing and verifiable reports of incidents of crime, public safety concerns, or other compelling circumstances are required to proceed. This does not include anecdotal evidence or speculation. The purpose of the proposed CCTV system must be clear, and the use of CCTV must be necessary to address the specific incidents or problems which have been identified. This means that less privacy-invasive measures must be evaluated, and where practical, implemented, to see whether the issue can be addressed through such measures, prior to the installation or usage of a CCTV system. Less privacy-invasive measures should be utilized unless they are ineffective or not feasible.

The following are other essential considerations for making a decision to decide whether or not to use CCTV in a school:

1. **Has the impact of the proposed CCTV system on privacy been assessed?**

   A Privacy Impact Assessment of the proposed CCTV system should be conducted at the school, not just the school district level, to determine the actual or potential kind and degree of interference with privacy that will result, and the ways in which adverse effects will be mitigated.

2. **Has the public (including parents, teachers, students and other stakeholders) been consulted?**

   It is recommended that public consultation be conducted with relevant stakeholders, including representatives of communities that will be affected. Prior to the installation of CCTV systems, schools and/or school districts should notify individuals, including students, parents/guardians, volunteers and staff of the intention to consider installation of CCTV. The specific rationale for a CCTV system should be explained, and there should be an opportunity to ask questions and debate other ways in which both privacy and security can be protected and maintained while addressing the issues which gave rise to the decision to explore the use of CCTV. Schools and/or school districts should also be able to explain the legal authority for the collection of personal information through CCTV. Notification should consist, at a minimum, of a memo to affected individuals, and posting of the information on the school and school district website(s). Public meetings with parents are also suggested, however it is also important to give students a

separate venue to provide their input and ask questions. Any written notices or memos should outline the principal purpose(s) for which CCTV is intended to be used and the name, title and contact information of someone who can answer questions about it. Regardless of the outcome of the consultation, schools and school districts must still be able to support the use of CCTV on the basis, as noted above, that there is a real, pressing and substantial problem which is ongoing in nature that has not and cannot be mitigated by other less privacy intrusive measures.

3. **Is the CCTV system consistent with applicable laws including *ATIPPA*?**

CCTV systems must be consistent with all applicable laws, including overarching laws such as the *Canadian Charter of Rights and Freedoms* and the *ATIPPA*.

4. **Has the CCTV system been designed to minimize the impact on privacy?**

The surveillance system should be designed and operated so that the privacy intrusion it creates is no greater than absolutely necessary to achieve the system's goals. For example, limited use of video surveillance (e.g., for limited periods of day, peak periods when problems have typically occurred) should be preferred to always-on surveillance if it will achieve substantially the same result. Furthermore, cameras should be limited to only those locations which are necessary to address the problem(s) identified as the rationale for CCTV in the school.

5. **Has the public been advised that they will be under surveillance?**

The public (including students, teachers and other staff) should be informed with clearly written signs at the perimeter of surveillance areas, which advise that the area is or may be under surveillance, and indicate who is responsible for the surveillance, including who is responsible for compliance with privacy laws, and who can be contacted to answer questions or provide information about the system.

6. **Does the school have fair information practices in place for the collection, use, disclosure, retention and destruction of personal information?**

The information collected through video surveillance should be minimal; its use should be restricted, its disclosure controlled, its retention limited, and its destruction assured. If a camera

is manually controlled or actively monitored, the recording function should only be turned on in the event of an observed or suspected infraction. If an unmonitored camera records continuously, the recordings should be conserved for a limited time only, according to a retention schedule, unless a serious incident has been captured or the recordings are relevant to a criminal act that has been reported to the police. Information collected through video surveillance should not be used for any purpose other than the purpose that law enforcement or another body with legal authority to do so has explicitly authorized. Any release or disclosure of recordings should be documented.

7. **Does the CCTV system eliminate or minimize excessive or unnecessary intrusions on privacy?**

Surveillance cameras should not be present in areas where people have a heightened expectation of privacy: for example, into windows of buildings, showers, washrooms, change rooms, etc. If cameras are adjustable by an operator, reasonable steps should be taken to ensure that they cannot be adjusted or manipulated to capture images in areas that are not intended to be under surveillance.

8. **Are the CCTV system operators sensitive to privacy issues?**

The operators of surveillance systems, including operators hired on contract, should be fully aware of the purposes of the system, and fully trained in rules protecting privacy. Operators and users of the CCTV system and recordings should sign confidentiality agreements.

9. **Are there assurances that the security of the equipment and images is protected?**

Access to the system's controls and reception equipment, and to the images it captures, should be limited to persons authorized in writing under the school's policy. Recordings should be securely held, and access within the organization limited to a need-to-know basis.

10. **Are the rights of individuals to have access to their personal information respected?**

People whose images are recorded have a right under *ATIPPA* to request access to their recorded personal information, including their image recorded by CCTV. Severing the personal

information in a recording (including software to implement blurring or blocking of the identities of others) may be necessary to allow individual access. Policies and procedures must accommodate such requests.

11. **Is the CCTV system subject to compliance review and evaluation?**

The system's operations should be subject to a regular compliance review and evaluation intended to identify any unintended negative impacts on privacy. In ideal circumstances a compliance review and evaluation should be conducted by persons or organizations independent of the management and direction of the video surveillance system. However, if financial challenges associated with contracting an external third party to do this work would prevent or unreasonably delay it, it is recommended that internal compliance reviews be conducted where external independent compliance reviews are not available. Compliance reviews should ensure compliance with the *ATIPPA* as well as the policy governing the system, including ensuring that only pertinent information is collected, that the system is used only for its intended purpose, and that privacy protections in the system are respected. Evaluation should take special note of the reasons for undertaking surveillance in the first place, as determined in the initial statement of the problem and the public consultation, and determine whether video surveillance has in fact addressed the problems identified at those stages. Evaluation may indicate that a video surveillance system should be terminated or reduced in scope, either because the problem that justified it in the first place is no longer significant, or because the surveillance has proven ineffective in addressing the problem. Evaluation should take into account the views of different groups in the community (or different communities) affected by the surveillance. Results of compliance reviews and evaluations should be made publicly available.

12. **Does the school and the school district have an explicit policy on the use of CCTV surveillance?**

As described above in the section entitled "Collection of Personal Information Using CCTV Surveillance," a comprehensive written policy governing the use of the surveillance equipment should be developed.

13. **Is there a mechanism in place to notify the public that the CCTV system has been adopted?**

Schools and school districts should recognize that individuals will want information about video surveillance systems. They may seek to know, for example, who has authorized the recording, whether and why their images have been recorded, what the images are used for, who has access to them, and how long they are retained. Schools and school districts should be prepared to provide this information.

Use of a Video Surveillance System on Busses

While all the general guidelines for the use of CCTV systems should also be adhered to when utilizing surveillance on school buses, it is also important to note that when contracting with independent bus drivers and/or bussing companies it is crucial that service agreements with any third party hired to conduct the surveillance or otherwise handle the surveillance equipment or records must be in place. Employees of the contractors must be made aware of the privacy restrictions in place and should be required to sign confidentiality agreements. School or school district-operated bussing systems should employ the same confidentiality requirements as would be in place for any school or board employee that has access to CCTV equipment or recordings.

Designing, Installing and Maintaining a Video Surveillance System

The CCTV surveillance system should be set up and operated to collect the minimum amount of information necessary to effectively achieve its intended purpose. This helps reduce the intrusion on individuals' privacy. Specifically, we recommend that:

- Cameras that are turned on for limited periods in the day are preferable to "always on" surveillance.
- Cameras should be positioned to avoid capturing images of individuals in areas which are not being targeted.
- Cameras should not be present in areas where people have a heightened expectation of privacy, for example, showers, bathrooms, change areas, staff rooms or into windows. Steps

should be taken to ensure that cameras cannot be adjusted or manipulated by the operator to capture images in such areas.

- Sound should not be recorded unless there is a specific and demonstrable need to do so. Sound recording represents an additional and even more significant layer of privacy intrusion, and therefore a decision to consider recording sound must follow a rigorous analysis. Sound recording should not be viewed as a routine element of CCTV.

Wireless technology poses additional security and privacy risks and should not be employed unless all necessary precautions are taken. Wireless video surveillance systems, or wireless CCTV, typically refer to systems that transmit wireless signals to television monitors, not computer screens. Commercially available systems do not normally have privacy or security designed into the transmission of the signal. As a result, such systems are easy to install but may allow unauthorized access unless special precautions are taken. Wireless transmissions like CCTV broadcasts are inherently subject to interference and interception, especially when they use publicly available frequency bands. CCTV signals are generally not encrypted or secured, and may easily be captured by others with an appropriately tuned receiver. As there are only a limited number of transmission channels, the chances of inadvertent interception are high.

As a general rule, wired solutions are more secure than wireless solutions due to the reduced likelihood of interception. If a wired solution is not available, or if wireless is required for some other purpose, then the School Board and School are responsible for ensuring that the security provisions of the system meet privacy requirements. The best way currently available to prevent the viewing of intercepted messages is by utilizing an encrypted, or scrambled, signal.

Notification and Signage After CCTV Installation

After installation and at the beginning of each school year schools and school districts should notify and inform individuals including students, parents/guardians, volunteers and staff of the legal authority for the collection of personal information; the principal purpose(s) for which the personal information collected through CCTV is intended to be used and the name, title, and contact information of someone who can answer questions about that collection. Notification should

consist, at a minimum, of memo to affected individuals, and posting of the information on the school and school district website(s).

Students, staff and the public should be notified, using clearly written signs, prominently displayed at the perimeter of the video surveillance area, of CCTV equipment locations, so that each person has reasonable and adequate warning that surveillance is, or may be, in operation. At a minimum, there should be a sign in place that notifies individuals of the recording and informs them that they may contact the school office with any questions.

Use of Video Surveillance Records

Information collected through CCTV surveillance should only be used for the purpose for which that surveillance has being undertaken. In other words, there must be a clear and specific rationale for installing CCTV, and personal information gathered through CCTV should only be used for purposes directly connected with that rationale. Schools and school districts should have clearly defined policies and procedures for the use of CCTV surveillance records. The school and school district is responsible for the content of the policies and procedures, including meeting the minimum standards as set out in these Guidelines.

Any information obtained through CCTV surveillance systems may only be used for purposes set out in the school's policies and procedures and must relate to the protection of students, staff and the public, or it must assist in the detection and deterrence of criminal activity and serious vandalism. Information should not be retained or used for purposes other than those described in the policy. For example, CCTV installed to prevent ongoing vandalism after school hours should not be used to deal with matters of routine school discipline during the school day.

Policies and procedures established by the schools and school districts should:

- Clearly state who can view/use the information and under what circumstances it may be viewed/used. The number of persons who may view the recorded information should be limited to specific individuals, such as the school Principal and a designated alternate (such as the Vice Principal).

- Ensure that circumstances warranting a review of recorded CCTV images should be limited to instances where a serious incident has been reported/observed or to investigate a potential crime.
- Provide that where real-time viewing of the monitors takes place, the authority to view the monitors may only be delegated by the principal to a limited number of individuals.
- Provide for logs of who accesses, uses or otherwise views information.
- Establish that electronic logs be kept if the technology to do so is available.
- Clearly state that CCTV surveillance should not be used for monitoring staff performance.

Disclosure of Video Surveillance Records

Personal information must not be disclosed except in accordance with *ATIPPA*. Because CCTV surveillance systems create a record by recording personal information, school districts with a CCTV system should implement written policies and procedures and ensure that these are adopted and followed by schools.

Policies and procedures established by the schools and school districts should:

- Clearly state who is responsible for deciding to disclose images or other information from CCTV systems and under what circumstances these images or information may be disclosed.
- Provide for logs of who the information is disclosed to and for written confirmation of receipt of the information by the person who has received it.
- Clearly state that CCTV surveillance images can only disclosed in compliance with the *ATIPPA*.

Retention of Video Surveillance Records

School districts should have clearly defined policies and procedures for the retention of CCTV surveillance records. The school district is responsible for the content of these policies and procedures, including meeting the minimum standards as set out in these Guidelines.

All recorded images must be stored in a secure location, and access should be granted only to a limited number of authorized individuals. All recordings that are not in use should be stored securely in a locked receptacle located in a controlled-access area. Each storage device that has been used should be dated and labeled with a unique, sequential number or other verifiable symbol.

Policies and procedures established by the schools and school districts should:

- Ensure that logs are kept of all instances of access to, and use of, recorded material, to provide for a proper audit trail.
- Set out the retention period for information that has not been viewed for the purpose of protecting student safety or to deter, detect, or assist in the investigation of criminal activity. Recorded information that has not been used in this fashion should be routinely erased according to a standard schedule. Unused recordings that are not viewed should be erased on a schedule not exceeding one month. The relevant retention periods should be clearly documented in both the school and school district policy and in the procedures;
- Establish a separate retention period when recorded information has been viewed for the purpose of protecting student safety or to deter, detect, or assist in the investigation of criminal activity. The length of this retention period may be established by the school and school district but should not exceed a reasonable period for which the personal information may be used for the aforementioned purpose.
- Require the school and school district to store and retain storage devices required for evidentiary purposes according to standard procedures until the law enforcement authorities request them. A storage device release form, or an entry in a logbook, should be completed before any storage device is disclosed to the appropriate authorities. The form should indicate who took the device, under what authority, when this occurred and if it will be

returned or destroyed after use. This activity should be regularly monitored and strictly enforced.

- Establish that electronic logs should be kept where records are maintained electronically.

Disposal of Video Surveillance Records

Recordings should only be kept as long as necessary to fulfill the purpose of the CCTV surveillance. Recordings no longer required should be destroyed. School districts and schools must ensure that the destruction is secure.

Policies and procedures established by the schools and school district should:

- Establish who is responsible for ensuring the safe and proper disposal/destruction of storage devices.
- Ensure that old storage devices must be securely disposed of in such a way that the personal information cannot be reconstructed or retrieved. Disposal methods could include overwriting electronic records, shredding, burning or magnetically erasing the personal information.
- A storage device disposal/destruction form, or an entry in a logbook, should be completed before any storage device is disposed of and/or destroyed. The form should indicate who disposed of/destroyed the device, under what authority, when this occurred and what method of destruction/disposal was utilized. This activity should be regularly monitored and strictly enforced.

Access to Personal Information

ATIPPA establishes that individuals have the right to access their own personal information, including their own images as recorded by CCTV. When disclosing recordings to individuals who appear in them, the school district must ensure that identifying information about any other individuals on the recording is not revealed. This can be done through technologies that mask identity.

Policies and procedures established by the schools and school district should:

- Clearly state who is responsible for deciding to provide access to the information and under what circumstances it was accessed.
- Provide for logs of who was given access to the information and when.
- Clearly state that CCTV surveillance is accessed for a specific purpose and is to be used only for that purpose.

Privacy Impact Assessment

The Office of Public Engagement defines a Privacy Impact Assessment (PIA) as a formal evaluation of the privacy implications within a specific project. The term "project", in this context, is very broad; it refers to a project, program, initiative, legislation, system, application, program, or any other defined course of endeavor. It elaborates by stating that a PIA is a comprehensive process for determining the privacy, confidentiality and security risks associated with the collection, use or disclosure of personal information. It may also define the measures used to mitigate and, wherever possible, eliminate the identified risks.

The Government of Newfoundland and Labrador's *PIA Policy* states:

"Public Bodies within the Government of Newfoundland and Labrador will conduct PIAs for all new and significantly redesigned collections, uses or disclosures of Personal Information that may raise potential privacy risks."

The OIPC strongly urges all School Districts and individual schools that are contemplating the use of CCTV systems conduct a PIA prior to reaching a decision on the installation of a CCTV system.

Reviewing and Evaluating the Use of Video Surveillance

Boards and schools should ensure that the use and security of video surveillance equipment are subject to regular compliance reviews and evaluations. These compliance reviews and evaluations should also address the institution's compliance with operational policies and procedures. An external body may be retained in order to perform the audit where possible. Any deficiencies or concerns identified by the audit must be addressed as soon as possible.

Employees and service providers should be aware that their activities are subject to such a review and that they may be called upon to justify their use of CCTV surveillance.

Boards and schools should regularly review and evaluate the CCTV surveillance program in order to ascertain whether it is still justified in accordance with the requirements. This should include an assessment of whether the deployment of cameras at a particular school remains justified, or whether CCTV programs should be decreased or increased in scope. This evaluation should occur in a timely manner.

Tips for limiting the privacy impact of a CCTV system:

- Only install cameras in problem areas identified at the time the decision was made to proceed with CCTV. For example, if the justification for CCTV was vandalism to outside school grounds or the outside of the school building, there may be no need for cameras inside the school.
- Activate cameras only during those times when the problems which led to the CCTV installation have occurred or are likely to occur in order to deal only with the identified problem. If there has been damage to the inside of the school due to break-ins on evenings or weekends, only turn on the cameras after school. That way, the CCTV will capture the image of anyone who has broken in to vandalize or steal from the building, but will not impact the privacy of staff or students. If there have been criminal activities or serious

vandalism inside the school building, when do these activities normally occur? If these problems generally occur after regular school hours during extracurricular activities when parts of the school are not occupied, turn on the cameras for those periods of time only.

- The Office of the Information and Privacy Commissioner is available to consult with schools and school districts at any time. As the oversight body for *ATIPPA*, we are in a position to make recommendations to help ensure compliance with that law, and we are willing to work with all stakeholders to help ensure that privacy can be protected while meeting other operational and security needs.