OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

The Use of Video Surveillance in Schools and on School Buses

Newfoundland and Labrador English School District

December 6, 2018

Table of Contents

Page #

Commissioner's Message

The *Access to Information and Protection of Privacy Act, 2015* (*ATIPPA, 2015*) limits the capacity of public bodies' to collect and use personal information in order to ensure the public's right to privacy. Privacy is a right that is recognized by the Supreme Court of Canada and is protected by the *Canadian Charter of Rights and Freedoms*. Video surveillance has long been a topic of interest for this Office, with guidance pieces on the topic dating back to 2013.

Video surveillance is becoming more and more prevalent in today's society and continues to erode our privacy. Many have become desensitized to its presence, assuming that someone is always watching or recording what we do. The implications of constant surveillance, especially ubiquitous surveillance of our children, are deserving of further research.

The foundations for acquiescence to omnipresent video surveillance include the opinions of those who hold the view that, *if you are not doing anything wrong, why should you care*. Beyond failing to recognize our constitutional right to privacy, this attitude fails to recognize that with advances in facial recognition technology, our participation in any event will be identifiable. Who decides what is 'wrong' in the face of the new reality that simply participating in a lawful protest or attending a political event might negatively impact your future prospects for employment, government assistance or other benefits.

The issue, in the context of schools, emerged into the spotlight in May 2017 when a media outlet reported the live streaming on a Russian website from video surveillance cameras installed in a school in Nova Scotia. Closer to home, the provincial NL Master Specification Guide for Public Funded Buildings, including schools, include CCTV capabilities. While it might make financial sense to pre-wire for potential future installation of CCTV or install CCTV systems during the construction of a building, doing so presents challenges for privacy. The Master Specifications do not appear to consider the *ATIPPA, 2015* when making decisions about surveillance systems and, in the case of new schools, accountability for *ATIPPA, 2015* compliance rests with the District. Newly constructed buildings, including schools, are being equipped with large numbers of cameras by default and many public bodies are using the cameras without a thought to their need or the requirement to evaluate whether their use accords with the *ATIPPA, 2015*.

It is important to note that with all cameras, not just the ones in newly constructed buildings, absent authority for the collection under the *ATIPPA, 2015*, public bodies collecting personal information using cameras are in fact breaking the law.

Video surveillance is not a tool that can be used in isolation and, in fact, research does not support video surveillance as a deterrent. Research does support the *perception* that video surveillance is a deterrent. While surveillance footage may be useful in investigating

incidents that have already occurred, the presence of the camera generally does not *prevent* the incidents in the first place.

This Office and the District are both committed to the creation of a safe and caring learning environment for students in our schools. To protect students in schools, video surveillance may have a role to play alongside other initiatives. While there are times that the use of video surveillance is justified, it should always be one of a number of alternative initiatives considered and/or implemented to address the issue at hand. During the course of this audit, for example, some schools documented alternate activities extremely well, including an entire school community, including parents and students, being re-educated on behavioral expectations, and trained school prefects monitoring the school during the day. Less privacy-invasive options must always be considered and explored before resorting to video surveillance.

When cameras are used, the *Act* requires that a clearly defined purpose be identified. Evidence and documentation to support the need for surveillance are required, including: specific incidents tied to each camera location to justify the use of each individual camera, and details of alternates considered and implemented prior to the camera use. Such documentation must be a living document, changing as needs arise and kept up to date. Anecdotal data is insufficient. Schools need to keep records of incidents of concern and track frequency before and after any preventative measures.

We hope that the District will use this audit as an opportunity to continue its evaluation of currently installed video surveillance systems to ensure that it has the authority, under the *ATIPPA, 2015,* to collect personal information via every camera/system operating in its schools. The District is legally obligated to cease collecting personal information if camera use cannot be justified. Further, no new cameras/systems are permissible until the District assesses and documents them as necessary.

We hope that students, parents and school associations will engage with the District in exploring the root causes of issues and the consideration of graduated responses to resolve problems that exist. The safety of students and staff is paramount. While video surveillance may sometimes be necessary to achieve that result, considerations must include interim responses that least impact privacy.

Donovan Molloy, Q.C.
Information and Privacy Commissioner
Newfoundland and Labrador

Executive Summary

The Office of the Information and Privacy Commissioner (OIPC) is an independent Office of the House of Assembly with oversight of the *Access to Information and Protection of Privacy Act, 2015* (*ATIPPA, 2015*) and the *Personal Health Information Act* (*PHIA*). Citizens expect the OIPC, as the oversight body, to assess the level of compliance with the law, to advocate for best practice and to assist public bodies in establishing effective privacy management programs.

To assist in these efforts, the OIPC has developed an Audit and Compliance Program. Audits are conducted under the authority of section 95(1)(b) and section 95(3) of the *ATIPPA, 2015*. Section 95(1)(b) empowers the Commissioner to *monitor and audit the practices and procedures employed by public bodies in carrying out their responsibilities and duties under this Act*. Section 95(3) extends the Commissioner's investigative powers established elsewhere in Part IV to other activities, including audit.

This is the third comprehensive audit undertaken by the OIPC.

While past audits have focused on establishing the expectations of this Office with regard to specific aspects of the *ATIPPA, 2015*, the expectations of this Office regarding video surveillance in schools are set out in our *Guidelines for the Use of Video Surveillance Systems in Schools,* released in February 2013. After the release of this guidance document, a number of school boards in the province merged to form the Newfoundland and Labrador English School District (NLESD or the District) in September 2013. The purpose of this audit was to assess compliance with the *ATIPPA, 2015* and the OIPC's guidance documents regarding video surveillance.

The use of video surveillance by the District was identified as an audit topic because of the potential to impact a large number of individuals, with approximately 67,000 students and 8,000 staff. Video surveillance also impacts the public as the cameras often capture anyone on or near school grounds within camera range. The NLESD issued a policy and affiliated procedures/regulations in 2014 that reflect the requirements of the *ATIPPA, 2015* and the guidance on video surveillance issued by this Office. However, this Office's pre-audit inquiry to determine if there were any gaps revealed areas of non-compliance, and it was decided to launch an audit.

This audit examines the collection, use and disclosure of personal information through the use of video surveillance, as well as the reasonableness of safeguards in place to protect same. In particular, this Office examined the District's authority for the collection, the purpose for collection, the notification of the collection and the safeguards in place to protect personal information collected via video surveillance.

During the course of the audit, the District addressed some of the identified gaps. For example, as public bodies are expected to know what personal information is being collected, the District has developed a database of video cameras for each school that is updated as new installation or expansion requests are received and processed. The District has also developed standard notification signage and made it available to schools and the annual inspection form used by District Facilities Division staff now includes a check for sufficient signage for all schools with video surveillance systems.

There are a number of concerns that remain outstanding. For example, the available documentation does not justify the use of many of the cameras currently in place and does not clearly outline other activities considered prior to determining that cameras were needed. In addition, the trend of installing and using a high number of cameras without any demonstrated justification in new builds is concerning. While installing video surveillance capabilities in new builds makes fiscal sense in the event it is needed in the future, the same considerations for activation and use of the system should apply.

Further, this Office has concerns regarding the District's authority to collect personal information using video surveillance. The District argues that collection of personal information using video surveillance is directly related to and necessary for an operating program or activity as per section 61(c) of the *ATIPPA, 2015*. The District's submission indicates that video surveillance is primarily used to ensure safety of students and staff, as well as to protect District property assets. While this Office agrees that the collection of personal information can be helpful in specific applications when creating a safe learning environment, it is not always necessary to ensure a safe learning environment or to protect assets.

Public bodies are also expected to protect the personal information in its custody and control. In general, a combination of administrative, physical and technical safeguards are used. Although a Preliminary Privacy Impact Assessment (PPIA) regarding video surveillance was conducted by the former Eastern School District in 2008, no review or updating of this document has occurred. While the NLESD established a video surveillance policy in 2014, instances of non-compliance were identified during the course of this audit. Administrative safeguards that are not kept up-to-date or enforced provide a false sense of security.

While the District advises that no cameras are currently used on buses, they have been used in the past and may be contemplated in the future. When this Office inquired about any contractual language regarding the use of cameras on buses, the District indicated that there is currently no language in contracts with bussing companies to address camera usage. The District indicates that the contract template is approved by the Department of Education and Early Childhood Development and it cannot be changed unilaterally. This is

a concern for this Office, as contractual language regarding the use of video surveillance on buses is a common administrative safeguard.

The District's submission identified a number of common technical safeguards, many of which appear on its new application form for video surveillance systems. However, incomplete application forms were approved and others were approved with question marks on the form. The District has also confirmed it does not have, and has not identified the capacity to outsource, the blocking or blurring of identities in videos prior to providing access.

The audit included 10 recommendations to address the identified gaps; the District has accepted all recommendations.

This Office recognizes the challenges facing schools and agrees that schools should be safe learning environments. While this Office supports the use of video surveillance in appropriate circumstances, it should not be the first or only solution utilized. Further, while many believe that surveillance cameras are a deterrent, the literature does not support this conclusion. It is imperative that public bodies understand that failing to adhere to the requirements of the *ATIPPA, 2015* is a violation of the law.

Introduction

The Office of the Information and Privacy Commissioner of Newfoundland and Labrador (OIPC) provides independent oversight of the *Access to Information and Protection of Privacy Act, 2015* (*ATIPPA, 2015*) and the *Personal Health Information Act* (*PHIA*).

The OIPC's Audit and Compliance Program includes evaluating the collection, use and disclosure of personal information, the adequacy of public body safeguards to protect personal information, and compliance with the *ATIPPA, 2015*. Audits are conducted under the authority of section 95(1)(b) and section 95(3) of the *ATIPPA, 2015*. Section 95(1)(b) empowers the Commissioner to *monitor and audit the practices and procedures employed by public bodies in carrying out their responsibilities and duties under this Act*. Section 95(3) extends the Commissioner's investigative powers established elsewhere in Part IV to other activities, including audit.

Citizens expect the OIPC, as the oversight body, to assess the level of compliance with the law, to advocate for best practice and to assist public bodies in establishing effective privacy management programs.

The Commissioner selected the Newfoundland and Labrador English School District (NLESD or the District) for audit after a pre-audit inquiry regarding the status of video surveillance. The response of the NLESD to the pre-audit inquiry revealed potential gaps in compliance that this Office determined warranted an audit into the matter. The use of video surveillance by the District has the potential to impact a large number of individuals, with approximately 67,000 students and 8,000 staff. The cameras will also capture anyone on or near school grounds within camera range.

Audit Objectives

The key objectives of this audit are to examine the following within the context of video surveillance:

- Examine compliance with the *ATIPPA, 2015* and the OIPC's guidance documents regarding video surveillance;
- Examine training provided to staff with access to information collected using video surveillance pursuant to the District's video surveillance policy;
- Identify any risk factors in the collection, use, disclosure and protection of personal information using video surveillance; and
- Make recommendations to strengthen NLESD policy and practice regarding video surveillance.

The lines of inquiry for this audit comprised whether the NLESD:

- Is authorized to collect personal information via surveillance cameras;
- Has met its obligations under the *ATIPPA, 2015* relating to policies and practices, consent and the collection, use, disclosure, and retention of personal information collected using video surveillance; and
- Protects personal information collected via video surveillance as required by section 64 of the *ATIPPA, 2015*.

Audit Focus

This audit encompassed any video surveillance that occurs in NLESD schools or on buses, including buses on contract with the District. This includes covert surveillance on District property since June 2014, even if District cameras were not used.

The NLESD was formed on September 1, 2013. While any surveillance equipment currently in use is within the scope of this audit, this Office appreciates that historical data (pre-2013) may be difficult to locate and would not have been encompassed by the current NLESD policy.

The scope of the audit is similar to the scope of the NLESD's policy – the use of video/electronic security systems in and around all schools and school buses owned, operated or contracted by NLESD. Video surveillance used on District assets other than schools and buses, such as the NLESD Headquarters on Elizabeth Avenue, is not in scope. This audit also does not examine recordings of specific events (such as a sporting event or graduation ceremony) or where a class may be recorded for educational or research purposes.

While other public bodies, such as the Department of Education and Early Childhood Development and the Department of Transportation and Works, are out of scope, consideration has been given to any directives or guidance provided to the District regarding video surveillance, as well as any requirements established for new construction of schools in the province.

Overview of Video Surveillance

This audit examines the collection, use and disclosure of personal information through the use of video surveillance, as well as the reasonableness of safeguards in place to protect same. In particular, this Office examined the District's authority for the collection, the purpose for collection, the notification of the collection and the safeguards in place to protect personal information collected via video surveillance.

ATIPPA, 2015

The NLESD is a public body as defined in section 2 of the *ATIPPA, 2015*. Section 2(x)(iv) establishes that a public body means a local public body and section 2(p)(i) establishes that a local public body means an educational body. Section 2(h)(v) establishes that an educational body means, "a school board, school district constituted or established under the Schools Act, 1997…"

Section 2(u) defines personal information as "recorded information about an identifiable individual." It is important to note that it is not an "identified individual" but rather an "identifiable individual." By using video surveillance and recording same, the NLESD is gathering or acquiring personal information. The District's Video Electronic Security Systems policy states that, "Personal information is recorded information about an identifiable individual, as defined in the ***Access to Information and Protection of Privacy Act***. Recorded information includes photographs, film and videotape." As such, the use of video surveillance is a collection of personal information where they record images/pictures.

Video Surveillance and Schools in Newfoundland and Labrador

In 2012, this Office undertook a survey of schools. At that time, there were five districts; Eastern, Nova Central, Western, Labrador and conseil scolaire francophone provincial de Terre-Neuve-et-Labrador. All districts reported some presence of video surveillance at that time, and this Office investigated the use of video surveillance at one school after a privacy complaint was received regarding same. After reviewing the results of the survey, researching best practice and consulting with the Districts, the Newfoundland and Labrador Teachers' Association, the Department of Education (currently the Department of Education and Early Childhood Development), and the Newfoundland and Labrador Federation of School Councils, this Office issued the OIPC *Guidelines for the Use of Video Surveillance Systems in Schools* in February 2013.

This guideline states, in part:

> *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 NLESD was formed on September 1, 2013, after our guidelines were released. The NLESD subsequently issued its own video surveillance policy in September 2014. The *Video Electronic Security Systems* policy establishes the District's support for the use of systems, "…on district property and in vehicles owned, operated or contracted by the District, where it is deemed necessary to protect the safety and security of students, staff and visitors and to protect student and district property." The Policy directive states that the systems are intended to complement and not replace other forms of monitoring and supervision.

During pre-audit inquiries, this Office asked the NLESD for an inventory of video surveillance cameras. Public bodies are expected to know what personal information is being collected, including information being captured on cameras. As the NLESD participated in a 2015 OIPC survey involving the use of video surveillance in public bodies, the District questioned why a new inventory was needed. The OIPC indicated that, as long as NLESD was satisfied with the accuracy of its contents, we would accept the 2015 results. The District elected to request that all schools complete a new survey.

Since our launch of this audit, the District has developed a database of video cameras for each school that is updated as new installation or expansion requests are received and processed. The District confirms that it continues to utilize and update this database and it is helpful in assessing video camera usage in schools. In order to ensure compliance with the *ATIPPA, 2015*, each public body must be aware of the personal information it collects, as well as how it is handled and stored. The District's new database is an important component of compliance.

What is the identified purpose for the collection?

It is best practice to collect the minimum amount of personal information required for the identified purpose; the *ATIPPA, 2015* only authorizes public bodies to use and disclose the minimum amount of personal information required to accomplish the identified purpose. Video surveillance can capture additional information, even where appropriate considerations are made. For example, if a school experiences vandalism on the exterior of the building outside of school hours, the cameras should only be on the exterior of the building and use should be restricted by either the time of day, motion detection and/or the angle of the cameras. Even with these mitigation activities, the cameras will not be able to discern between two children playing near the school versus two individuals vandalizing the school. As such, irrelevant and unnecessary personal information will be collected even in well-planned surveillance situations. This adds to the importance of

attempting to address concerns using other means before resorting to video surveillance. Further, public bodies should not collect personal information for one purpose and use it for another.

Although individual schools are implementing video surveillance systems, they are not public bodies under the *ATIPPA, 2015*. The District is the public body collecting personal information using video surveillance, having custody or control of the records, and ultimately accountable for this activity under the *ATIPPA, 2015*. Through policy, the District has assigned responsibility of these systems to school administrators. As such, all school administrators should be aware of the specific reason for collecting personal information via video surveillance. The spreadsheet provided by the NLESD identified a variety of purposes for the collection. Unfortunately, some schools indicated that they were unsure or unaware of the purposes of installing video surveillance or merely indicated new construction as the reason. A number of schools noted that it was District protocol, part of a secure schools initiative, or cited the Safe and Caring Schools Policy. In the absence of specific reasons, the use of video surveillance should be re-evaluated. Further, while the NLESD may delegate certain responsibilities regarding CCTV to schools administrators, the head of the NLESD remains accountable for *ATIPPA, 2015* compliance.

Some schools listed particular student safety issues, including student runners (students prone to leaving school quickly without permission) and fights, as well as general safety issues, such as a shooting at a nearby building and an abduction attempt. One school indicated it installed cameras after two fires were set in a washroom. These types of specific examples are capable of validating the use of *specific* cameras for well-defined purposes.

Many cited building security, specifically the monitoring of fire alarms, bomb threats and entrance security. Other schools cited additional illegal activities including theft, break-ins, drug use and vandalism. It is more difficult to determine if camera use is appropriate without links to camera locations and details regarding the number and timing of specific incidents.

As the District was only formed in 2013 and there is turnover among school administrators, this Office appreciates that historical information may be difficult to locate. To obtain a better understanding of how video cameras contribute to safety, we asked the District about the role video surveillance played during specific threats that closed schools, required RNC involvement and were reported in the media during the course of this audit. The District indicated:

> *The role video footage plays in the safety and security of students is typically more routine than high-profile incidents reported in the news. It is the day-to-*

day aggressive student behaviors that results in school-based discipline, or the monitoring of access to the school and school grounds. For example:

- *Video footage was used this year to identify a man who entered a St. John's high school and allegedly sexually assaulted a student;*
- *Video footage was used to identify two individuals who had accessed a high school with a student, but had no cause to be at the school. The two individuals in question were known to law enforcement, and were in breach of an undertaking to have no contact with each other.*
- *It was used to discipline students who had bullied another student – pulling his pants down to his knees in the school hallway.*
- *It was used to discipline students observed using a vaping device in school.*
- *It was used to determine, and confirm the accounts of, witnesses to a lunch-hour fight and deal appropriately with the students involved.*
- *It was also used to determine the instigator of a fight that broke out in the corridor of a Western region high school as students were transitioning to classes.*
- *It was used to determine which students had ripped a soap dispenser from a wall and spread soap over the floor, endangering others students.*
- *Video footage is used to ensure individuals identified as being prohibited from being around certain children, or any children, are not accessing the school or school grounds.*

These are just a few examples reported to us for the purposes of responding to your question. Principals indicate that the most important way video surveillance is used to address student (and staff) safety within our schools, and on school grounds, is by acting as a ***deterrent*** *to even more violence, aggression and theft. One principal noted that with respect to bullying complaints, video surveillance drastically reduces investigation time. It enables school staff to intervene more quickly and efficiently, which is of benefit to the victims. It was also reported that theft from lockers has been drastically reduced since video surveillance was installed.*

This Office recognizes the challenges facing schools and agrees that schools should be safe learning environments. While this Office supports the use of video surveillance in appropriate circumstances, it should not be the first or only solution utilized. Further, while many believe that surveillance cameras are a deterrent, the literature does not support this conclusion. In 2017, the Nova Scotia OIPC issued Investigation Report IR17-01; this Report examined the use of Video Surveillance at the Cape Breton-Victoria Regional

School Board. As part of this report, the OIPC NS conducted a literature review of video surveillance in schools. In summarizing a review conducted by the Ontario OIPC in 2008, the report commented, "The one firm outcome was that the literature supports video surveillance as a useful tool for producing evidence that can be used to help investigate an incident after the incident has occurred."

The questionable status of video surveillance as a deterrent is mentioned again in the Report's conclusion, which stated in part:

> *[197] Privacy is fundamental to allowing individuals the space to grow, develop and live as autonomous and contributing members of a thriving democracy. Academic research on the effectiveness of video surveillance to be a proactive safety tool is, at best, mixed. But researchers are clear on the impacts video surveillance has on individual's sense of themselves: they negatively impact how trusted they feel, of how respected they feel and of how free they are.*

The OIPC's Guidelines, when discussing purpose for collecting personal information using video surveillance, states:

> *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?*

In this regard, this Office would like to highlight the application for a new installation submitted by one school. The school applied for eight cameras in total, with specific hours of operation identified. The school included a floor plan with clearly marked camera locations, both interior and exterior, and a list of specific incidents that lead to the request for cameras. Two typed pages containing specific details were included with the application. The school identified a number of alternatives employed prior to considering cameras, stating:

> *We have attempted to increase/improve student accountability, we consistently refer to and employ our school code of conduct. We have continuously made parent contact and engaged in problem solving discussions with our school council. We have increased supervision, we formed and supported a student prefect group – who model desired behavior, we do regular washroom checks, and we have individualized plans to support students who exhibit challenging behavior.*

By comparison, another newly constructed elementary school requested 30 cameras (interior and exterior) to provide 24 hour surveillance. Three specific incidents were identified, all of which happened in a two week time period in specific areas of the school. The only alternate activity undertaken was supervision. The information provided on this application does not establish the necessity of 30 cameras operating 24 hours a day. The District questioned the appropriateness of comparing a school that came with 30 cameras installed as part of the government tender issued to construct the school to an existing school requesting to install eight cameras. While this Office recognizes the substantial differences in the two situations, the standards for using video surveillance should be the same in both new builds and existing schools. Students attending school, whether in an older structure or a new build, have the same right to privacy and the District has the same obligations under the *ATIPPA, 2015*.

While this Office appreciates the importance of a safe learning environment, it cannot support the collection of personal information using video cameras where doing so is not established as necessary within the meaning of the *ATIPPA, 2015*. Further, the use of video surveillance should be one of a number of activities considered. In isolation, video surveillance is unable to provide a safe learning environment.

It is positive to note that applications for expansion of current systems generally contain details of specific incidents and link the camera locations to those incidents. In addition, the District has approved several applications in part, refusing to allow cameras in certain locations.

Authority to Collect

District's Submission

Given that over collection is practically inevitable with video surveillance, establishing the authority to collect personal information using this tool is essential. The *ATIPPA, 2015* addresses the purposes for which public bodies may collect personal information in section 61:

> *61. 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.*

The District is relying on section 61(c) of the *ATIPPA, 2015* as the authority for the collection; it argues that collection of personal information using video surveillance is directly related to and necessary for an operating program or activity. The District's submission indicates that video surveillance is primarily used to ensure safety of students and staff, as well as to protect District property assets. The District has a mandate to promote a safe and caring learning environment. The use of video surveillance for safety reasons is the primary identified purpose cited by school administrators.

The *Protection of Privacy: Policy and Procedures Manual* produced by the ATIPP Office discusses interpretations of section 61(c) on page 21:

> ***2.2.3 Relates Directly to and is Necessary for an Operating Program or Activity (paragraph 61(c))***
>
> *Paragraph 61(c) permits a public body to collect personal information where that information relates directly to and is necessary for an operating program or activity of the public body.*
>
> ***Relates directly** to means that the personal information must have a direct bearing on the program or activity.*
>
> ***Necessary for** means that the public body must be able to demonstrate a need for the information being collected.*
>
> *In assessing whether personal information is "necessary", the sensitivity of the personal information must be considered including the particular purpose for the collection and the amount of personal information collected and assessed in light of the purpose for collection. [Order F07-10, Information and Privacy Commissioner of British Columbia]*
>
> *An **operating program** is a series of functions designed to carry out all or part of a public body's operations. An **activity** is an individual action designed to assist in carrying out an operating program.*

To show that the collection of personal information with a video surveillance system is authorized by the *Act*, the District would need to:

(a) relate the collection of information using video surveillance to an operating program or activity of the District, and
(b) show that the information being collected is necessary.

In its submission, the District states:

> *Video security at schools and on school buses is primarily to help ensure the safety of students and staff, as well as to protect public investment in property owned by Newfoundland and Labrador English School District. The mandate of the elected Board of Trustees of the District is outlined s. 75(1) of the Schools Act, 1997, which includes implementing curriculum and educational programs, human resources, finance and operations, facilities maintenance and student transportation.*
>
> *Under the Act, a school board is also specifically required to:*
>
> - *determine policy for the effective operation of primary, elementary and secondary education within the district [s. 75 (1)(c)], and*
> - *promote a safe and caring learning environment for schools in the district [Sec. 75(1)(c.1)*
>
> *The Director of a school district is also required, under the direction of the Board, to promote a safe and caring learning environment for schools in the district [Sec. 80(l.1)].*
>
> *A school principal is required to:*
>
> - *manage the school [s. 24(3)(e)];*
> - *promote a safe and caring learning environment [s.24 (3)(e.1), and*
> - *maintain order and discipline in the school and on the school grounds and at those other activities that are determined by the principal, with the teachers at the school to be school activities [s. 24(3)(f)]*
>
> *The District is further required to comply with the Provincial Government's Safe and Caring Schools Policy (2013), s. 2.7 of which refers to elements of a safe school, including:*
>
> - *an environment free from bullying, harassment, intimidation and discrimination*
> - *an orderly environment; and*
> - *security procedures which are resistant to intrusion.*

The Department of Education and Early Childhood Development has established a Safe and Caring Schools Initiative, "to promote safe and caring learning environments and to be proactive/preventative in addressing violence issues." While there is no mention of video

surveillance in the Safe and Caring Schools Policy, there are brief mentions in the evaluation report prepared in 2012. The *Report on the Evaluation of the Department of Education's Safe and Caring Schools Policy and its Implementation* states, in part:

> *Goal 1: To improve the culture and climate within the school*
>
> *Objective 1.2: Improve students' sense of belonging and well-being within our school*
>
> *Strategies:*
> *…*
>
> - *1.2.3 Address student safety on buses and around our building by holding meetings with bussing companies and installation of video monitoring system.*
>
> *Success indicator: Less incidents around school and on busses.*

While the District has anecdotal evidence of fewer incidents after the installation of video surveillance, it does not appear that such data is tracked with the requisite detail.

The same report, under section 14 (effective practices), states:

> *14.11 Attend to safety issues for critical incidents*
>
> *Ensure there are regular lockdown, bus and fire drills.*
>
> *Have designated safe places in the school where students can go when they are feeling threatened or under attack. Have staff available to ensure the safety of those who come to this site.*
>
> *High school students supported this focus on safety noting that key aspects of supporting their school to be safe and caring school included hall monitors and sufficient numbers of staff monitoring activities in all areas of the school/strong supervision processes, on-site video cameras and the front door being locked (with doorbell entry) during school hours.*

Although the Report mentions high school students' support for video surveillance in response to critical incidents, cameras are installed in schools with all age levels. Furthermore, there is no indication of whether students support a particular level of CCTV or whether it is necessary at all schools, inside or outside, certain times of day, etc.

The District's submission did not identify other steps taken to comply with the Safe and Caring Schools Policy, although many individual applications for video surveillance listed substantial alternative actions considered prior to applying for video surveillance. When discussing considerations prior to undertaking video surveillance, the *Guidelines for the Use of Video Surveillance Systems in Schools* state, in part:

> - *privacy-specific criteria that must be met before CCTV surveillance is undertaken including a description of alternative measures undertaken and their results;*
> - *documentation of the decision, including a detailed rationale and purpose for the surveillance;*

The Case Law

The Ontario OIPC examined the authority to collect personal information using video surveillance in school settings in Privacy Complaint MC13-46. This Report addressed one parent's concerns with the use of video surveillance at a school and states, in part:

> *In Cash Converters Canada Inc. v. Oshawa (City) [Cash Converters Canada Inc. v. Oshawa (City), (2007) 86 O.R. (3d) 401] the Ontario Court of Appeal adopted the following approach with respect to the application of the necessity condition and stated:*
>
> > *In cases decided by the Commissioner's office, it has required that in order to meet the necessity condition, the institution must show that each item or class of personal information that is to be collected is necessary to properly administer the lawfully authorized activity. Consequently, where the personal information would merely be helpful to the activity, it is not "necessary" within the meaning of the Act. Similarly, where the purpose can be accomplished another way, the institution is obliged to choose the other route. [Ibid, at para. 40]*
>
> *This approach was adopted in Special Investigation Report, MC07-68 and Privacy Complaint Report MC10-2 and incorporated into the Guidelines. In Special Investigation Report, MC07-68, Commissioner Cavoukian concluded:*
>
> > *Based on the test established by my office, and adopted by the Court of Appeal, in order to satisfy the necessity condition, the institution must first identify the "lawfully authorized activity" in question, and second, it must demonstrate how the collection of personal information is "necessary," not merely helpful, to the achievement of*

> *this objective. In addition, this justification must be provided for all classes of personal information that are collected.*

The Information and Privacy Commissioner of British Columbia discussed the meaning of "necessity" in the context of the collection of personal information in Order F07-10:

> *[48] The collection of personal information by state actors covered by FIPPA - including local public bodies such as the Board - will be reviewed in a searching manner and it is appropriate to hold them to a fairly rigorous standard of necessity while respecting the language of FIPPA. It is certainly not enough that personal information would be nice to have or because it could perhaps be of use some time in the future. Nor is it enough that it would be merely convenient to have the information.*

Even if there are reasons to employ video surveillance as part of the District's programs, each collection of personal information (i.e. each individual camera in each school) must also be necessary within the meaning of section 61(c). Our Guidelines state:

> *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.*

OIPC Review

Based on the above standard, while this Office agrees that the collection of personal information can be helpful in specific applications when creating a safe learning environment, it is not always necessary to ensure a safe learning environment. Further, the relationship between video surveillance and a safe learning environment is not always clear. As referenced in the previous section, there are, of course, exceptions to this.

The District recognizes the need to balance safety with privacy when using video surveillance:

> *The District is mindful of individuals' right to privacy – whether they are students, staff, or the public. We must, however, balance that right with the requirement to provide a safe, secure teaching and learning environment for all, and to use available means and resources to meet that obligation. The District has determined that in order to meet the requirements of the Act and the provincial Safe and Caring Schools Policy, the use of video security can be an effective means of monitoring access to the school; responding to incidents of bullying/harassment, vandalism and theft, and serving as a deterrent to negative/criminal behaviours. As such, the elected Board of Trustees exercised its authority to develop and implement a policy. The policy, along with associated administrative procedures/regulations, was implemented in September 2014.*

It is also important to address the impact that surveillance in schools has on children. In October 2012, the Office of the Privacy Commissioner of Canada released a report titled, *Surveillance Technologies and Children*. The Report concluded:

> *The coming together of societal, technological and commercial factors have caused technological surveillance of children to be commonplace in our society. Since this is a relatively recent phenomenon, the effects of this pervasive surveillance on children are only beginning to be studied. Available research has raised legitimate questions about the potentially detrimental effects surveillance may have on children's social development in the long term. Some have posited that growing up with surveillance as a daily presence may even normalize the practice over time and influence a shift in social norms away from privacy.*

New Builds

Some of the applications provided to this Office involved newly constructed schools. New construction of government buildings is subject to standards established by the Department of Transportation and Works, which are mandatory for building contracts tendered for the Department. The NL Master Specification Guide for Public Funded Buildings was compiled by the Department of Transportation and Works and reviewed by a committee of industry representatives. Video surveillance standards are established in the Closed Circuit Television section and it is the understanding of this Office that, while some school administrators have been involved in the location of cameras, not all are. It is important for the public body that will ultimately be accountable for collection of personal

information using the cameras to be involved in the identification of camera locations and usage of same.

The District's submission indicates that including video surveillance capabilities in new builds has complicated the application process, commenting, "Administrators did not feel the need to apply to use them [video surveillance system], any more than they would apply to use any equipment installed in their school." This Office appreciates the cost efficiency of new construction having video surveillance capabilities. However, there is nothing requiring public bodies to use any or all of the cameras installed. On this point, the District submits:

> *In recent years, the Provincial Government has included the installation of video surveillance systems in tenders for some newly-constructed schools and major redevelopments. Given this reality, it is the District's view that it is incumbent on us to ensure the equipment is utilized for the purposes outlined in our policy statement. The District would be poorly positioned if called upon to explain why a multi-million dollar building with a complete CCTV system had no recorded evidence if a serious incident was to occur. We have a responsibility to protect public investment in District-owned properties.*

In Order P-09-02, the OIPC of British Columbia examined the issue of surveillance cameras and new construction. In this complaint, residents complained about aspects of use of video surveillance in their condominium, governed by the Shoal Point Strata Council. While this case revolved around BC's private sector legislation, the *Personal Information Protection Act*, it discusses relevant standards when examining video surveillance and new construction.

The Report states, in part:

> *[63] Shoal Point asserts that ensuring security is an appropriate purpose for using video surveillance. It did not, however, provide any evidence of legitimate security concerns that existed prior to the implementation of the surveillance.*
>
> *[64] Based on the parties' submissions, it appears that at least eight of the cameras were installed while the complex was being built. It seems that they were incorporated into the building design and were put into use once the building opened. This means that the original decision to implement the surveillance was taken before there was any evidence of security threats. There might have been evidence at the time the building was constructed that would lead to a reasonable expectation that there would be break-ins at*

the main entrances, but Shoal Point did not provide any such evidence in its submission. In other words, it appears there was merely an assumption, as yet unsupported, of any security threat.

[65] Several years after the building was occupied, there were incidents of theft as the result of unauthorized entry from a service door that was not subject to surveillance. There were also two incidents of unauthorized entry into the parkade and four incidents of accidental damage to the building caused by vehicles in the parkade. The decision to install video cameras in these areas was taken in response to these incidents.

…

[71] The other striking point of this case is the paucity of substantial evidence to justify Shoal Point's implementation of video surveillance. Other than the installation of cameras by the service door and in the parkade, Shoal Point's implementation of video surveillance has been pre-emptive, not in response to demonstrated problems. The reported incidents that have occurred are not exceptional and are spread over several years.

[72] Decisions about whether to implement video surveillance should not be swayed unduly by the general appeal of technological solutions. They should be based on an assessment, in the circumstances of each case, of the real need for surveillance of this kind, its reasonably expected benefits and the impact of its use on privacy. Video surveillance should be used only in response to a real and significant security or safety problem. In saying this, I note as an aside that one of the inherent risks of video surveillance is "function creep", which is the extension of the uses of a technology beyond the use for which it was implemented in the first place. There are cases, for example, in which surveillance cameras originally installed to deter burglary were subsequently used to enforce minor infractions. [Information and Privacy Commissioner of British Columbia, Investigation Report P98-012: Video Surveillance by Public Bodies: a discussion (March 1998)]

[73] I do, however, find it significant that the incidents of unauthorized entry leading to theft occurred through doors that originally were not subject to video surveillance. This suggests that video surveillance at the other doors might have deterred the perpetrators. Therefore, I conclude that, if the incidents of unauthorized entry justified the reactive implementation of video surveillance at some of the external doors, it would be reasonable to retain the cameras previously installed by the other external doors.

The District notes that they now ask administration in newly constructed schools to apply to the District to use the video surveillance in their schools. Although the NLESD policy has always required approval prior to using such systems, we appreciate how administrators could have misinterpreted this in newly constructed buildings. The District explained that many assumed that all provided systems could be used without additional approval.

The Office recognizes that valid reasons for using all or part of a video surveillance system from day 1 at a newly constructed school MAY exist. During this audit, an application for one newly constructed school made an argument based on past experience (the school population will move from the current school to the new location) and vandalism and thefts that occurred during off hours during the construction phase. These points justified at least some of the surveillance installed and used in the new facility.

No matter if video surveillance capabilities are standard in new construction, the same considerations for activation and use of the system apply.

Notification

When collecting personal information, section 62(2) of the *ATIPPA, 2015* states:

> *A public body shall tell an individual from whom it collects personal information*
> *(a) the purpose for collecting it;*
> *(b) the legal authority for collecting it; and*
> *(c) the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.*

NLESD policy reflects this legislative requirement, stating, "Signs shall be prominently displayed advising that a video/electronic security system is/may be in operation." The affiliated procedure/regulation states:

> *2.1 Once a video/electronic security system is approved, notification must be provided in writing to the school council, parents/guardians and employees, that a system is approved for use and the expected start date of operation.*
>
> *2.2 When a video/electronic security system is installed on a bus, written notice must be provided to the parents/guardians of students who regularly use that bus.*

> *2.3 Signs advising that a video/electronic surveillance system is/may be operating must be displayed at entrances to buildings, at the front of school buses and in all areas that are subject to surveillance.*
>
> *2.4 At the beginning of each school year, students and parents/guardians shall be informed of the use of a video/electronic security system through the normal means of communication (e.g. newsletter, school website, memo home).*

OIPC Guidelines for the Use of Video Surveillance Systems in Schools states:

> *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.*

The survey conducted by the District in Fall 2017 revealed that a number of schools and buses do not have notifications in place regarding the use of video surveillance. This is contrary to both NLESD policy and the *ATIPPA, 2015*. At least two of the schools with no notices have shared copies of video footage with law enforcement and at least one includes cameras with audio capabilities (the District indicates that the audio feature is not in use at any school). Furthermore, some schools with a high number of cameras have only one notice. For example, a school with 35 cameras, another with 29 cameras, and one with 18 cameras (17 of which have audio capabilities), all with only one notice each.

During the course of this audit, the District took several steps to address this issue. A January 2018 memo from the Associate Director (Programs and Operations) included a template for interior signage; a template for exterior signage is in development. In addition, District Facilities Division staff formally inspect all schools once a year. The

inspection form now includes a check for sufficient signage for all schools with video surveillance systems.

Protection of Personal Information

Public bodies collecting personal information must establish that reasonable safeguards are in place to protect the information. The reasonableness of safeguards is discussed in detail in OIPC's Audit of Physical Safeguards, issued in June 2016. The *ATIPPA, 2015* states, in part:

> *64. (1) The head of a public body shall take steps that are reasonable in the circumstances to ensure that*
>
> *(a) personal information in its custody or control is protected against theft, loss and unauthorized collection, access, use or disclosure;*
>
> *(b) records containing personal information in its custody or control are protected against unauthorized copying or modification; and*
>
> *(c) records containing personal information in its custody or control are retained, transferred and disposed of in a secure manner.*

In general, public bodies use a combination of administrative, physical and technical safeguards to protect the personal information in its custody and control. Each will be discussed in turn.

Administrative Safeguards

A Privacy Impact Assessment (PIA) is a recognized tool that assists in evaluating new and changed initiatives for privacy impacts, risk mitigation and legislative compliance. A Preliminary PIA (PPIA) regarding video surveillance was conducted by the former Eastern School District in 2008. This document states, in part, "Many schools in Eastern School District have video surveillance systems in place, and many more desire to add them. We would like an "umbrella" assessment of video surveillance systems, with site-specific analyses to be conducted with this as a framework." It does not appear that site-specific analyses were conducted, although the NLESD has an application process in place that is addressing this gap on a go-forward basis.

PIAs generally have a review schedule. In addition to a specific review timeframe, changes can prompt a review. In the 10 years since the PPIA was developed, the Eastern School District became part of the NLESD, the *ATIPPA* was replaced by the *ATIPPA*, *2015*, and video surveillance technology has changed. Any one of these activities should have prompted a review.

Another common administrative safeguard involves policy and procedures. The NLESD's current video surveillance policy came into force on September 1, 2014. The District was asked about resources prepared to complement the policy and any education or promotion done when the policy was released. The policy, while new to the NLESD, was developed from existing policies at the former Boards with which administrators were already familiar. The policy was disseminated to schools and placed on the website. As new systems were approved, a letter or e-mail was sent to the administrator with a link to the policy/regulations and a reminder of some of the key requirements. The District's submission also identified other activities:

> *The District also developed and disseminated ATIPPA FAQs (which includes a section on video surveillance) for the 2014-15 school year, and updated/reissued them in 2015, 2016 and 2017. This information remains available on a Principal Resources Team Drive online. Presentations on ATIPPA, including a section on video surveillance, were presented at leadership (principals) meetings in 2015. The video security policy has also been included in ATIPPA presentations provided to those enrolled in the District "Emerging Leaders" program for the past two years.*
>
> *Note: The OIPC notes the District has recently developed new standard signage and provided draft text for administrators to consider when informing their school communities about video surveillance. Schools, which had video security systems prior to school board consolidation, had similar resources provided when they were approved for cameras under the authority of their previous school boards.*

Once an application to expand or install video surveillance is received at the District, it is reviewed by the ATIPP Coordinator and the Director of Facilities to identify any concerns with rationale, privacy, and camera location. The Associate Director of Education (Programs and Operations) makes a final decision. Within the past year, the District has started to require schools to submit a floor plan indicating camera locations, as well as requiring newly constructed schools to submit an application. The District has also worked on updating the existing database of information on video security systems in schools.

Although the District's Video Electronic Security Systems policy has been in place since 2014, instances of non-compliance were identified during the course of this audit. For example, NLESD policy requires that the District be notified when a school provides a copy of footage to a third party. The District states, "The District acknowledges that schools have not been adhering to the regulation stipulating that the District must be notified when copies of surveillance footage is shared (typically with law enforcement)."

The District is encouraged to make efforts to ensure that schools are in compliance with policies and procedures. The District's submission stated, "Information provided to your office in 2015 and 2017 provided the District an opportunity to follow-up with schools where compliance issues were identified (e.g. cameras inappropriately located; no applications on file; insufficient signage). That work continues." This Office encourages the District to continue with these efforts, as, in the absence of compliance checks and enforcement, it is difficult for public bodies to demonstrate that they have reasonable administrative safeguards in place.

Another common administrative safeguard is training. While this Office recognizes the difficult task facing the District when it comes to training 8000 staff, not all staff will require the same level of training when it comes to video surveillance. This Office has higher expectations of staff with access to the video surveillance footage and camera control features, for example. During the course of the audit the District inquired as to assistance available from this Office. One of the duties of the Commissioner under section 95(1)(b) is to, …"inform public bodies of their responsibilities and duties, including the duty to assist, under this Act." While this Office can train staff on the *ATIPPA, 2015*, it is not able to train staff on the policies and procedures developed by the public body.

This Office discussed in-person training with the District, as well as a short written piece on privacy considerations when using video surveillance in schools. We also welcomed other suggestions that could leverage communication tools already in use by the District.

Technical Safeguards

The District's submission identified a number of common technical safeguards, including user names and passwords, single points of connection and firewalls. The survey conducted earlier this fall indicated that 14 schools are able to remotely access cameras. When the District follow-up with these schools, all indicated that it was a misunderstanding. The District has confirmed that no schools are currently able to remotely access their cameras.

The new application form for video surveillance includes security questions, such as:

- Who will have access to the Video/Electronic Security System Monitors?
- How will surveillance recordings be stored/saved?
- Is/will the system be connected to the computer network?
    - If yes, has access to the system been confirmed as restricted by the NLESD IT Department?

Responses to the first question generally indicate restricted access, for example many include administration or simply the principal and vice-principal. This restricted access appears to be a reasonable safeguard.

When it comes to saving and storing the recordings, the majority of recordings are saved and stored on systems that came with the surveillance system, on a special hard drive or on the District's system. This Office has some concerns over the completeness of some forms, as four of the eight that answered "yes" to the question "Is/will the system be connected to the computer network?" did not respond to or answered "no" to the follow-up question, "If yes, has access to the system been confirmed as restricted by the NLESD IT Department?" Further, at least one that answered "no" indicated that the recordings will be stored on a "hard drive in system." While there was a question mark next to this response in pen, there are no further details on whether the District followed up on this discrepancy.

Finally, the majority of schools have indicated that they have viewed video surveillance footage. Schools indicated that footage has been viewed by principals, vice-principals, school administrators, parents, students and law enforcement. Of those, 33 indicated they have shared a physical copy of video surveillance footage. The *ATIPPA, 2015* requires that the minimum amount of personal information necessary to accomplish the identified purpose be used and disclosed. While not a technical safeguard, there is a technical solution for this issue in the form of software that can block or blur the identities in videos prior to providing access. When asked about it, the District stated, "the District has not employed any such software."

Report A-2018-005, released by this Office during the course of this audit, states:

> *Even if portions of the recordings captured the personal information of identifiable individuals, that fact would not automatically preclude disclosure pursuant to the ATIPPA, 2015. De-identification of individuals by blurring/pixelating their images could allow disclosure of the recordings. Ontario Report MO-3358 addresses a very similar scenario. After retaining an outside agency to de-identify persons captured by video cameras belonging to the City of Ottawa, disclosure of the recordings was no longer an unreasonable invasion of the personal privacy of the people recorded. Our Guidelines for Video Surveillance by Public Bodies recommend that public bodies have this capacity. A lack of technical or other capacity to use in-house personnel may require outsourcing de-identification requirements.*

Video Surveillance on Buses

In the response to the pre-audit inquiry dated August 22, 2017, the NLESD provided information regarding video surveillance on school buses within the jurisdiction of the NLESD. In its submission, the District surveyed all bus companies under contract and advised that none were using interior cameras. One contractor was using exterior surveillance that had been part of a pilot project initiated by the Department of Education and Early Childhood Development; as the pilot project is currently inactive, the District advised them to disengage the cameras. The District also noted that a contractor was using a dashcam and directed them to remove it. The District's submission indicates, "With respect to buses, please note that the District has decided to disengage all interior/exterior cameras at this time."

This Office inquired about safeguards regarding cameras on buses. The District noted, "There is no standard contract language in place specific to camera usage at this time. The District utilizes a contract template approved by the Department of Education and Early Childhood Development. It cannot be changed unilaterally." This is a concern for this Office, as contractual language regarding the use of video surveillance on buses would be a common administrative safeguard. In the absence of such language, the District may not have legal authority to direct a contractor on the use of video surveillance on buses under contract with the District. Further, the District, although accountable for collections of personal information, appears to have no control over the contractual language used.

The pilot project referred to above was implemented in 2012-13 to test the effectiveness of cameras in reducing the number of vehicles illegally passing school buses when their stop arms and lights are activated. No PIA was completed on the pilot project and it is currently inactive.

The use of video surveillance was addressed in an August 2013 report, *Student Transportation Considerations*, conducted by Deloitte; the OIPC was one of a number of stakeholders that was engaged to provide views and perspectives to Deloitte. Deloitte was engaged by the government to, "conduct an independent review and evaluation of the school transportation system with the view to providing valuable insight into how to enhance school transportations services, within existing budgets, with the needs and safety of students remaining the first priority."

Video surveillance was mentioned a number of times in the final report. The report indicates that there were approximately 34 school buses equipped with video surveillance. Although cameras would be able to monitor student behavior while the driver is focused on the road, conflicting opinions existed regarding parental support for cameras. In general, the report concluded that support existed for the use of cameras in specific circumstances. Deloitte acknowledged the OIPC Guidelines that suggest permanent

cameras on buses are not appropriate and should be used as a last resort. The report states:

> *It is Deloitte's opinion that Districts should adhere with these guidelines. In light of these guidelines, the report presents alternatives for Districts including student monitors, better training for drivers, and lastly, paid adult monitors.*

If cameras are being considered, the Report states:

> *In advance of any usage of cameras, detailed policies and procedures should be developed to outline creation, destruction, viewing and storage of confidential information.*

The Report states:

> *The Department is encouraged to look at implementing a student monitor program. Student monitors play an invaluable role should something happen to the driver. Student monitors are trained at using the bus two way communication system, evacuating a bus and sometimes even providing basic First Aid (depending on training). Student monitors can and do play an oversight role on the bus as well, again depending on the training provided. While the Districts have concerns that there may be some liability issues with student volunteers, the CAA, in partnership with the police, school boards and parents, have operated the Safety Patroller program for over 80 years in Ontario, so there are successful models that can be emulated. The Bus Patroller program currently has 25,000 elementary school Patrollers serving 800 schools in Ontario.*

As for implementation, the report states, as a long term goal (12 months plus):

> *Long term (12 months plus): The Department should investigate the training programs available for student monitors and consider their implementation. The Department, in conjunction with OPIC [sic], should ensure each of the Districts has appropriate policies and procedures on the creation, destruction, distribution, viewing and storage of confidential information including the use of cameras and monitors. The Department should consider expanding driver training requirements to better enable drivers to manage student behavior.*

Observations and Recommendations

Identified Purpose for Collection

By its very nature, video surveillance captures additional information, even where appropriate considerations are made. This adds to the importance of attempting to address concerns using other means before resorting to video surveillance and to clearly understand why the cameras are being used.

This Office recognizes the challenges facing schools and agrees that schools should be safe learning environments. Unfortunately, some schools indicated that they were unsure or unaware of why the video surveillance was installed, or merely indicated new construction as the reason. While this Office supports the use of video surveillance where necessary within the meaning of the *ATIPPA, 2015*, it should not be the first solution sought. Indeed attempting other solutions and assessing their impacts is part of the necessity evaluation. Further, it is difficult to determine if camera use is appropriate when the surveillance is not tied to specific incidents and evidence is lacking about whether alternate options were considered or explored.

As the District was only recently formed and there is turnover among school administrators, this Office appreciates that historical information may be difficult to locate. It is positive to note that applications for expansion of current systems generally contain details of specific incidents and link the camera locations to those incidents. In addition, the District has approved several applications in part, refusing to allow cameras in certain locations.

While this Office appreciates the importance of a safe learning environment, it cannot support the collection of personal information using video cameras where there is no justification for same. Further, the use of video surveillance should be one of a number of activities considered. In isolation, video surveillance is unable to provide a safe learning environment.

During the course of the audit, this Office inquired if there were plans to require all schools to complete forms for video surveillance. The District responded:

> *Schools that had camera systems prior to September 2013 applied/were approved under the policies, administrative procedures or practices of the previous school boards (Eastern, Nova Central and Western District all had policies and regulations published online. Labrador did not). The District has no plans to require schools to reapply to the "new" District. New procedures will come into effect as systems are changed or upgraded. At this time, with pressing demands on limited District resources, a large-scale retroactive application process would not be considered a priority use of staff*

> *resources, nor a priority use of a school administrator's time. It would be difficult to estimate how long such a process would take.*

While we appreciate the concerns of the District, public bodies must know the personal information they are collecting, using and disclosing, as well as the purpose for the collection. In the absence of such knowledge, it cannot be concluded that the public body is in compliance with the *ATIPPA, 2015.*

Recommendation

> The District should develop evaluation criteria based on the OIPC's Guidelines and implement an evaluation program during the 2018-19 school year. For schools that have previously submitted applications/documentation, either to former Boards or to the NLESD, in regards to the installation or use of video surveillance, the District should review that documentation to ensure the evaluation criteria are satisfied. For schools that have not submitted applications/documentation in regards to the installation or use of video surveillance, the District should require them to submit it and ensure the evaluation criteria are satisfied.

Public Body Response:

The District accepts this recommendation. The District's policy regarding the implementation/modification of CCTV systems requires the school to list examples of incidents predicating the use of video surveillance. This application requirement is consistent with OIPC Guidelines for Use of Video Surveillance in Schools - namely "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?" The District has begun a province-wide review of our CCTV documentation on a school-by-school basis. Our current review processes have been enhanced to include additional checks to confirm and document the identified need for CCTV versus other strategies to address concerns.

Authority to Collect

While this Office appreciates the District's attempt to balance privacy rights with the need to provide a safe, secure teaching and learning environment, the District has not demonstrated an overarching authority to collect personal information via video surveillance under section 61(c). That being said, it is the finding of this Office that there is potential for some individual schools to successfully argue that the collection of personal information via video surveillance is directly related to and necessary for the creation of a safe learning environment.

Recommendation

As the District has not demonstrated the general authority to collect personal information via video surveillance under section 61(c) of the *ATIPPA, 2015*, the OIPC recommends that it prohibit the installation of new cameras in existing schools and the use of cameras installed as part of the construction process in new schools, absent the submission and District approval of documentation establishing their necessity. The documentation should include a floor plan with camera locations. The District should reject proposed cameras unless it is satisfied they meet the necessity requirement.

Any cameras presently in use that were not previously approved by the District as meeting the necessity requirement must be assessed and approved by the District as satisfying the evaluation criteria. The District should use best efforts to complete this review of existing and new/revised documentation (where required) by December 31, 2019 and update the OIPC every 3 months on its progress.

Public Body Response:

The District accepts this recommendation. The District is confident, based on prior reviews, that CCTV is being used appropriately in schools as per relevant legislative requirements. CCTV is generally used to assist with providing physical safety to the school environment

(i.e.; curtailing vandalism impacting the building, and/or to support safe and caring schools by helping to ensure occupants are safe). That said, the District is in the process of determining which schools require further documentation to demonstrate compliance with 61(c) of ATIPPA, 2015 - "that information relates directly to and is necessary for an operating program or activity of the public body."

Notification

Both the *ATIPPA, 2015* and the District's policy require collection notices. However, the survey conducted by the District in Fall 2017 revealed that a number of schools do not have notifications in place regarding the use of video surveillance. Further, some schools with a high number of cameras have only one notice. For example, a school with 35 cameras, another with 29 cameras, and one with 18 cameras (17 of which have audio capabilities), all with one notice each.

During the course of this audit, the District took several steps to address this issue. A January 2018 memo from the Associate Director (Programs and Operations) included a template for interior signage; a template for exterior signage is in development. In addition, all schools are formally inspected once a year by District Facilities Division staff. The inspection form now includes a check for signage for all schools with video surveillance systems.

Recommendation

The District should continue with efforts to ensure appropriate signage is in place. The expectation of the OIPC is that the District use best efforts to ensure all instances of video surveillance have appropriate signage by June 1, 2019.

Public Body Response:

The District accepts this recommendation. Sign templates have been delivered to all schools, and their presence is being confirmed via an annual documented school inspection.

Recommendation

> NLESD ensure compliance with its own policy, which requires written notification to school council, parents/guardians and employees. It further requires communication (e.g. newsletter, school website, memo home) informing students and parents/guardians of the use of video surveillance at the beginning of each school year.

Public Body Response:

The District accepts this recommendation. Direction will be provided to each school with CCTV to ensure that the presence of the system is communicated home in the initial memo/newsletter to parents and guardians each year. The District will also provide professional learning to administrators with respect to their responsibility to notify the school community when a video surveillance system is present in a school.

Protection of Personal Information

Public bodies collecting personal information are expected to ensure reasonable safeguards (technical, administrative and physical) are in place to protect the information.

Administrative Safeguards

Although the Eastern School District completed a PPIA in 2008, much has changed since that time. A new, province-wide District was created, the *Access to Information and Protection of Privacy Act* underwent several revisions, the *Guidelines for Video Surveillance in Schools* was released, and the technology involved in video surveillance changed, with costs for equipment going down and quality of images improving. This and the passage of time since the initial PPIA should have prompted an updated assessment of the impact of video surveillance on privacy in the schools.

In 2014, the NLESD issued a robust policy and affiliated procedures/regulations that reflect the requirements of the *ATIPPA, 2015* and the guidance on video surveillance issued by this Office. The District communicated with staff regarding the policy when it was initially released and has provided reminders to staff.

However, this Office identified a number of areas of non-compliance with the policy during the course of this audit. Further, the District approved installations and expansions that

were accompanied by incomplete forms. Other forms contained comments and questions, with no indication if the District had received responses before approval was provided.

Recommendation

> The District conduct an updated assessment on the privacy impacts of its video surveillance program. This should be done in compliance with the PPIA/PIA Review Criteria issued by this Office.

Public Body Response:

The District accepts this recommendation. During the 2018-19 school year, the District will review the existing privacy impact assessment conducted by a predecessor District and update/revise as appropriate.

Recommendation

> NLESD develop a mechanism to better ensure compliance with NLESD policies and procedures/regulations.

Public Body Response:

The District accepts this recommendation. NLESD has recently begun offering online professional learning sessions to address questions and clarify current policies. The Video Electronic Security Systems policy will be added to these sessions. The District will also continue to utilize our database to allow better control and updating of individual school information regarding video surveillance in schools. The administrator's annual planner checklist has been updated to include a reminder to review the policy and ensure schools are in compliance. In addition, video surveillance in schools will be subject to periodic audit by our internal audit division and/or other District staff who are trained in the area of privacy protection. As per normal audit standards, the District will audit a fixed number of schools each year, and expand upon that number if/as required.

Recommendation

> NLESD continue with the newly adopted practice of attaching a form with comments and follow-up questions and answers to all applications.

Public Body Response:

The District accepts this recommendation. The District is updating the current application form to reflect the documented review that precedes formal approval, and will continue to require this form for all CCTV installations/modifications.

Technical Safeguards

The District's submission identified a number of common technical safeguards, including user names and passwords, single points of connection and firewalls. While access was generally restricted to a small number of people, some schools indicated a high number of individuals with access. It is also concerning that the District does not have software that can block or blur the identities in videos.

Recommendation

> NLESD develop further guidance regarding appropriate access to personal information collected using video surveillance to better ensure that the minimum number of people necessary have access.

Public Body Response:

The District accepts this recommendation. As indicated in response to a previous recommendation, the District will be commencing a privacy impact assessment process regarding CCTV in this school year. This process will serve to assist with determining and documenting who specifically requires access to records created by CCTV systems. This will also inform the content of future professional learning sessions related to ATIPP in general, and the Video Electronic Security Systems policy in particular. Again as indicated in response to a previous

recommendation, the District will also audit a select number of schools per school year.

Recommendation

> NLESD identify and obtain appropriate software, or identify a third party service provider, to block or blur identities of bystanders prior to disclosing videos other than to a law enforcement agency or in response to a summons, court order or other legal compulsion.

Public Body Response:

The District accepts this recommendation. The District will ensure compliance with the ATIPPA, and in particular the privacy of all individuals captured by CCTV systems, prior to disclosing - when and if we receive an access request. The District notes that while the recommendation envisages a technical solution, the release of video may be authorized without use of said technology, provided the proper consent is received from the affected parties.

Video Surveillance on Buses

While the District operates some school buses, others are under contract with the District. The District indicates that there is no contractual language regarding video surveillance on buses in current contracts. Further, the District indicates that, although party to the contracts, the language is provided by the Department of Education and Early Childhood Development.

Recommendation

> NLESD work with the Department of Education and Early Childhood Development to develop appropriate contractual language regarding video surveillance on buses and incorporate into contracts starting the 2019/2020 school year. Any such contract language should reflect the recommendation in the Deloitte report Student Transportation Considerations:

In advance of any usage of cameras, detailed policies and procedures should be developed to outline creation, destruction, viewing and storage of confidential information.

Public Body Response:

The District accepts this recommendation. In advance of CCTV being broadly or systematically implemented on school buses, the District will work with the Department of Education and Early Childhood Development on policy/procedures related to these systems. As contracts are initiated or renewed thereafter, the contract language will be revised to ensure compliance with both ATIPPA and internal policies and procedures.

Conclusion

Public bodies are expected to know what personal information is being collected, why it is being collected, and how it is being protected. These details are even more important when personal information is being collected using video surveillance, as the cameras may capture much more personal information than required for the identified purpose.

Although the NLESD had a number of safeguards in place, areas of non-compliance were identified during the course of the audit. This Office is pleased that the NLESD has accepted all recommendations in this Report and has started on implementation.

This Office encourages every public body to review the standards discussed in this Report and to conduct internal reviews to determine their own level of compliance.

Donovan Molloy, Q.C.
Information and Privacy Commissioner
Newfoundland and Labrador