Yukon
Information
and Privacy
Commissioner

3162 Third Avenue, Main Floor
Whitehorse, Yukon, Y1A 1G3
T: 867.667.8468
F: 867.667.8469
1-800-661-0408 ext. 8468
www.yukonombudsman.ca

PRIVACY COMPLIANCE AUDIT REPORT

File ATP-CMP-2022-01-020

Pursuant to section 111(1)(b) of the

Access to Information and Protection of Privacy Act

Diane McLeod-McKay

Information and Privacy Commissioner

Department of Education

June 14, 2022

Summary

After learning in February of 2022 that the Department of Education was using video surveillance technology (VST) to surveil the activities of students and other individuals, including teachers, parents and visitors, in some Yukon schools, the Information and Privacy Commissioner (IPC) decided to investigate the authority for its use and conduct a compliance audit to evaluate whether the personal information collected through its use of VST in schools is adequately protected in accordance with the requirements of the *Access to Information and Protection of Privacy* Act (ATIPPA)[1] and the *Access to Information and Protection of Privacy Act Regulation* (Regulation).[2]

This report contains the findings of the IPC's compliance audit. The primary focus of the compliance audit was to examine if the Department is meeting its obligation to adequately secure the personal information held in accordance with section 30 of the ATIPPA and section 9 of the Regulation (Security Measures).

In conducting the compliance audit, the IPC examined the Department's existing policies, procedures and practices for the use and disclosure of personal information collected as a result of using VST in a school and the storage, retention, and destruction practices as well the rules regarding access and for breach reporting and management. The IPC also evaluated certain specific security requirements, namely, who has access to this personal information and why, and the technical, administrative and physical controls that are being used by the Department to assure the confidentiality, integrity and availability of the records created as a result of using VST in schools (VST Records).

These policies, procedures and practices, and the technical, administrative and physical measures being used by the Department to secure the personal information in the VST Records were evaluated against the Security Measures.

After reviewing documentation provided by the Department, the IPC determined that the Department is not fully meeting its obligations under Section 30 of the ATIPPA and section 9 of the Regulation as it relates to its duties thereunder to have in place adequate policies, procedures and practices to protect the VST Records. The IPC also determined that the Department should

[1] SY 2018, c.9.
[2] O.I.C. 2021/25.

implement additional security measures to prevent unauthorized access to the VST Records and to adequately protect the confidentiality, integrity and availability of the personal information contained in the VST Records.

Contents

Explanatory Note

All sections, subsections, paragraphs and the like referenced in this Privacy Compliance Audit Report are to the *Access to Information and Protection of Privacy Act* (ATIPPA)[3] unless otherwise stated.

References to 'Regulation' are references to the *Access to Information and Protection of Privacy Regulation*, Order In Council 2021/25.

References to 'VS Policy' are references to the Department of Education's Video Surveillance Policy unless otherwise stated.[4]

References to the 'Department' are to the Department of Education unless otherwise stated.

References to "VST Record(s)" means personal information recorded through the use of VST in a school or that is otherwise created through its use of VST.

Compliance Audit Scope

Public bodies are obligated to adequately secure personal information held in accordance with section 30 of the ATIPPA and the relevant provisions of the Regulation. The Department is a public body that is subject to the ATIPPA.

Given that the personal information that is being collected by the Department in the VST Records is highly sensitive involving images of youth while going about their activities in school, I decided to conduct a compliance audit of the policies, procedures, practices and information security of this personal information that is being collected via VST or that is otherwise held by the Department as a result of its use of VST.

This compliance audit will examine, for any of the personal information that has or is being collected by the Department via VST and that is held by the Department, whether this personal information is properly secured in accordance with the requirements of ATIPPA and the Regulation, including:

1. the policies, processes or practices being used by the Department to:

    (a) prevent the unauthorized use or disclosure of this personal information;

[3] SY 2018, c.9; amended by SY 2019, c.15.
[4] Yukon Dept. of Education, Video Surveillance Policy, dated: Feb 6, 2017. Submitted Feb 2022.

(b) store this personal information;

(c) destroy this personal information;

(d) protect, manage and control access to this personal information;

(e) secure this personal information including while in transit; and

(f) manage breaches of privacy related to this personal information; and

2. how security of this personal information is being managed throughout its lifecycle including:

(a) who has access to the personal information and why; and

(b) technical, administrative, and physical controls that assure confidentiality, integrity, and availability in each step of the lifecycle.

This compliance audit is informed by my investigation into the Department's use of video surveillance technology (VST) in seven schools.[5] My findings in the VST Investigation Report[6] included that the Department did not establish that it has authority to collect personal information via VST.

Submission of the Public Body

[1] The Department made no submissions regarding the compliance issues as defined in the scope of the compliance audit.

[2] As part of their submissions package for the investigation, the Department provided documents that will be referenced as part of this compliance audit.

[5] Investigation Report, Department of Education, ATP-ADJ-2022-02-044, June 14, 2022 (VST Investigation Report), at para. 10 (YK IPC). [redacted]

[6] *Ibid.*

Compliance Audit

Policy, procedures, and practices

[3] The following issue will be examined to determine the Department's compliance with the security requirements under section 30 of the ATIPPA and section 9 of the Regulation for the personal information that it holds as a result of its use of VST.

What are the policies, processes or practices being used by the Department to:

- prevent the unauthorized collection, use or disclosure of the personal information;
- store the personal information;
- destroy the personal information;
- protect, manage and control access to the personal information;
- secure the personal information including while in transit; and
- manage breaches of privacy related to the personal information?"[7]

(Hereafter, the "Policies, Processes and Practice Issue")

[4] As indicated, the Department made no submissions for the purpose of this compliance audit, but it has included some relevant documents in the document package that I will refer to as they are relevant.

Relevant law

[5] Section 30 of the ATIPPA states:

The head of a public body must protect personal information held by the public body by securely managing the personal information in accordance with the regulations.

[6] Subsection 9 (1) Regulation states:

In section 30 of the Act and in this section

"protect", in relation to personal Information, means

[7] As per NOI letter – concatenation mine.

(a) to protect the confidentiality, integrity and availability of the personal information,

(b) to protect the personal Information from a privacy breach.

[7] "Privacy breach" is defined in the ATIPPA as "in respect of personal information, means the theft or loss of, or unauthorized use, disclosure or disposal of the personal information.[8]

[8] Subsection (2) of the Regulation states:

(2) For the purpose of section 30 of the Act, the head of each public body must establish and implement administrative, technical and physical security measures appropriate to protect the personal information of each type or class of personal information that it holds.

(3) The security measures established under subsection (2) must include the following:

(a) a written practice respecting privacy breaches that sets out the responsibilities of employees under sections 20, 24 and 31 of the Act and of designated privacy officers and heads of public bodies under section 32 of the Act;

(b) measures to protect the personal information against risks

(i) of inadvertent modification, or

(ii) of damage, corruption or unintended destruction,

(iii) of the Information inaccessible,

(iv) of unsecured storage, transmittal or transfer,

(v) of theft, loss or unauthorized use, disclosure or disposal, and

(vi) of any other threats or hazards that the public body expects may exist.

(4) In establishing and implementing security measures under subsection (2), the head of a public body must take the following into account:

(a) the types or classes of personal information that it holds;

[8] Definitions, section 1.

(b) the sensitivity of the personal Information of each type or class of personal information that it holds;

(c) for each type or class of personal information that it holds, the risk of harm, including significant harm, that may occur to an individual if the public body fails to protect the personal Information;

(d) the benefits and costs of alternative security measures.

…

(10) Subject to subsection (11), the head of a public body must ensure that a record of user activity is maintained in respect of each instance when an employee of the public body accesses personal information in an electronic Information system maintained by the public body.

(11) Subsection (10) does not apply in respect of an electronic information system obtained by a public body before the coming into force of that subsection.

[9] The Department is a Class A public body.[9] As such, it is obligated to comply with the following additional security requirements that are set out in the Regulation.

(13) In addition to meeting the requirements of subsections (2) to (6), (8) and (10) to (12), the head of each Class A public body must, with respect to the public body,

(a) establish or adopt written policies respecting the protection of the personal Information held by it;

(b) ensure that the effectiveness of its security measures is tested and evaluated on a periodic basis;

(c) modify its security measures as required to ensure the protection of the personal information held by the public body;

(d) update its security measures when necessary to comply with the Act and this Regulation;

[9] "Class A public body" is defined in the Regulation to include a 'ministerial body'. The ATIPPA defines a "ministerial body" to include "the department over which the minister responsible presides".

(e) establish a written information security strategy regarding the establishment and implementation of security measures under subsection (2) and the establishment of policies under paragraph (a);

(f) designate one or more employees of a public body, by position title, to be responsible for training employees of the Class A public body with respect to the Act and regulations;

(g) designate one or more employees of a Class A public body, by position title, to be responsible for monitoring its employees to ensure compliance with the Act and regulations;

(h) designate one of its employees, by position title, to be responsible for responding to inquiries about its security measures; and

(I) set out practices and procedures to effectively mitigate against risks to the secure management of the personal information that it holds that may arise from a service provider being given access to personal information held by it.

(14) In the case of a Class A public body that is a ministerial body, the policies referred to Jn paragraph (13)(a) are, collectively, a manual for the purpose of the application of subparagraph 39(a)(iii) of the Act."

(Collectively, the "Security Measures")

Analysis - Policy, procedures, and practices

[10] The VS Policy that went into effect on February 7, 2017, has not been updated to reflect the requirements in the new ATIPPA and Regulation.

Collection of the VST Records

[11] My VST Investigation Report sets out the requirements of the Department regarding the collection of personal information using VST. I will not repeat my findings herein. The Department should refer to my Report and incorporate the rules for collection as set out therein, noting that any collection of personal information using VST must also 'directly relate to' the purpose of collection. Incorporating these rules into the VS Policy will mitigate the risk of unauthorized collection of personal information as a result of using VST in a school.

Use of the VST Records

[12] The Department is prohibited by section 19 from, amongst other things, using personal information beyond the amount that is necessary to carry out the purpose to which the use relates.[10] It is also prohibited from using personal information unless it is authorized to do so under section 21. There are four provisions in this section that authorize the Department to use the personal information in the VST Records. They are:

1. if the use is for the purpose for which the personal information was collected (subsection 21 (a));
2. if the use is directly connected to the purpose for which the personal information was collected and is necessary for the Department to use the personal information for this purpose (subsection 21 (b));
3. if the use is necessary for the Department to prevent or reduce a serious threat to public health or safety, or to protect the health or safety of an individual (subsection 21 (d)); or
4. if the individual the information is about consents to the use (subsection 21 (e)).[11]

[13] The VS Policy says little about authorized uses of the personal information in the VST Records. It states "[i]nformation obtained through the use of video surveillance will only be reviewed when investigating an incident or a complaint".[12]

[14] In one PIA, it indicates that the personal information is used by the principal and the [redacted] based on a triggering incident.[13] The other identifies that it is used in cases of vandalism or bullying or threatening behaviour.[14]

[15] In the documents provided, there is evidence that the Department is using the VST records to discipline students and for other purposes.[15] The Department is only authorized to use the personal information that it collects via VST under subsection 21 (a) for the specific purpose of its activity, which is ensuring student and staff safety and security in schools, and ensuring the care

[10] Subsection 19 (b).
[11] Subsections 21 (a), (b), (d) and (e). Subsection 21 (c) is not relevant to this analyses.
[12] VS Policy, at p. 6.
[13] [redacted].
[14] [redacted].
[15] See Appendix A. Some of the documents provided indicate other uses including to help with law enforcement, monitor events inside and outside of the school, and to address bullying or threatening behavior.

and maintenance of school property (Activity).[16] This Activity does not on its own authorize the Department to collect any personal information that may be related to the Activity, the information must also be *necessary* for the Activity.[17]

[16] One of the factors that I identified in my VST Investigation Report in determining necessity for the use of VST in a school was that there must be a history of incidents involving the specific school that creates significant risks to the health or safety of students in the school or the risk of significant damage to school property to justify using VST in the school to record personal information. The necessity threshold, therefore, qualifies the purpose of collection for the Activity such that any subsequent use of the information under subsection 21 (a) is limited to the sole purpose of addressing significant and serious incidents that threaten the health or safety of students in the school or for addressing significant and serious damage to school property.

[17] Under subsection 21 (b). the Department may only use the personal information in the VST Records if the purpose of the use is directly connected to the purpose of addressing significant and serious incidents that threaten the health or safety of students in the school or for addressing significant and serious damage to school property and the use is necessary for the Department to carry out the Activity or perform a statutory duty.

[18] The Department can rely on subsection 21 (d) if the use of the personal information in the VST Records is necessary for the Department to prevent or reduce a serious threat to public health or safety or to protect the health or safety of an individual.

[19] Lastly, it can rely on subsection 21 (e) to use the personal information in the VST Records for any other purpose if the individual the information about consents to the use in the prescribed manner that is set out in section 7 of the Regulation.

[20] It is unclear to me if the Department has authority to use the personal information collected for discipline or the other matters that it identified in its document package. It will need to consider its authority for any use of the personal information in the VST Records should it recommence using VST in any of the seven schools identified in the Investigation Report. After making its determination, the VS Policy should be updated to clarify that the use of personal information in the VST Records is restricted by the rules in the ATIPPA regarding use. How it is restricted should be laid out in the VS Policy. It should also be clarified in the VS Policy that any use that is not authorized is a reportable privacy breach.[18] By incorporating these requirements

[16] See paragraphs 36 to 40 of the Investigation Report.
[17] See paragraphs 41 to 67 of the Investigation Report.
[18] See section 20.

into the VS Policy, and any others that the Department feels is relevant, the risk of unauthorized use will be mitigated.

Disclosure of the VST Records

[21] The rules regarding disclosure of the personal information in the VST Records is set out in sections 23 and 25 of the ATIPPA. Section 23 restricts the amount of personal information that may be disclosed to that which is reasonably necessary to carry out the purpose of the disclosure. Section 25 lists the only circumstances in which the personal information may be disclosed. Subsection 25 (a) limits disclosure to the purpose for which the personal information was collected. Subsection 25 (c) limits disclosure for a use that is directly connected to the purpose of collection and where it is necessary for the Department to carry out the Activity. There are a number of other provisions under section 25 that authorize disclosure including with the consent of the individual the information is about, which must be in accordance with the prescribed requirements for consent in the Regulation.

[22] The VS Policy makes reference to certain kinds of disclosures. One is to parents or guardians and students. The other is "to police to assist in police investigations as authorized by the ATIPP".[19] Both PIAs indicate that the personal information may be disclosed for the purposes of law enforcement or court proceedings.[20]

[23] It is unclear to me if the Department is authorized to make these kinds of disclosures. It will need to assess its authority should it recommence using VST in any of the seven schools.

[24] In order to prevent unauthorized disclosures of the personal information in the VST Records the VS Policy should contain the following information:

1. clarification that disclosures may only occur if permitted by the ATIPPA;
2. disclosures that are authorized for routine matters, such as, for example, disclosures, to parents, guardians or students and for law enforcement purposes and the rules associated with these disclosures, as derived from the ATIPPA, should be set out in the Policy; and

[19] VS Policy, at p. 6.
[20] [redacted]

3. a requirement that for any non-routine disclosure that permission be sought from a designated individual, whose role will be to ensure there is authority under the ATIPPA for the disclosure.

[25] I will note here that there is a section in the policy "Exceptional Circumstances" that states:

> *Upon approval of the Assistant Deputy Minister of Public Schools, in situations where the particular circumstances of a case are such that the provisions of this policy cannot be applied or to do so would result in an unfair or an unintended result, some or all of the provisions of this policy may be waived based on the individual merits and justice of the situation. Such a decision would be considered for that specific case only and would not be precedent setting.*
>
> *If this exceptional circumstances clause is utilized, the Assistant Deputy Minister of Public schools will, as soon as is reasonable, notify the Yukon Teachers Association, the Yukon Information and Privacy Commissioner, and any School Board or Council involved of the rationale for doing so.*

[26] Also, under the heading "Access and Review of Video Surveillance Records" it states that "[p]arents and/or guardians may, if authorized by the building administrator, review a segment of a recording if the segment relates to a specific incident (e.g., accident or misconduct) involving their child/children, unless the review might violate the privacy of a third party. In that case, the review shall not take place unless authorized by the Assistant Deputy Minister of Public Schools. My emphasis.

[27] It should be clarified in the VS Policy that under no circumstances can the ATIPPA be violated for any use or disclosure of the personal information in the VST Records and that there are offences for violations of the use and disclosure provisions.[21]

Storage and Retention

Storage

[28] The VS Policy references the storage of the personal information collected in the VST Records.

[21] See paragraphs 121 (1)(b) and (c).

1. "Storage device" is defined in the VS Policy as a "videotape, computer disc 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".[22]

2. Under "installation and use" it states "[o]nly designated Department of Education employees or agents, or the building administrator or delegate, shall install or handle a video surveillance camera(s) or storage device(s).[23]

3. Under "video surveillance records" it states "[a]ll information obtained through the use of video surveillance will be protected and handled in accordance with the requirements of the ATIPP."[24]

4. Under "access and review of video surveillance records" it states "[t]he storage device shall be password protected, encrypted and stored in a secure area".[25]

[29] One PIA indicated that the personal information is stored [redacted].[26] It elaborates later in the PIA that the images are stored [redacted].[27] [redacted].[28] [redacted].

[30] What I can infer from the evidence is the following:

1. [redacted]

2. [redacted]

[22] VS Policy., at p.2.
[23] *Ibid.,* at p. 3.
[24] *Ibid.*, at p. 5.
[25] *Ibid.*
[26] [redacted]
[27] *Ibid.*, at p. 11.
[28] *Ibid.,* at p. 12
[29] *Ibid.*

3. [redacted]

4. [redacted]

[31] It is unclear if the VST Records are stored on a dedicated drive that is access controlled or if they are accessible by any person who has access to the drive, which may be accessible by Department employees for other purposes.

[32] The documentation provided indicates that there is no documented process and [redacted] In practice there appears to be a deviation from the VS Policy, e.g., [redacted] Some schools do document restricted key-fob access to the room where the hard disks are stored.

[33] It is up to the Department to ensure that the personal information in the VST Records are adequately secured against unauthorized access, theft, loss, and unauthorized disclosure and against other risks such as inadvertent modification, damage or corruption or unintended destruction, or inaccessibility of the information, in accordance with the ATIPPA's requirements, which amongst other things require the Department to:

1. protect the information from a breach;
2. have written information security practices;
3. establish security measures that adequately protect the highly sensitive personal information;
4. have written policies regarding the protection of the personal information;
5. test and evaluate the security measures periodically;
6. modify the measures as needed to protect the personal information; and
7. have a written security strategy to implement the security measures and written information security policies.

[34] The Department has not provided sufficient evidence to demonstrate that the personal information in the VST Records is stored in such a manner that it is adequately protected. It has not provided any written policies, procedures or practices to support the same.

[35] To bring itself into compliance with the requirements in the ATIPPA and Regulation for security of the storage device, as indicated it will need to develop and implement written information security policies and practices that are adequate to protect the VST Records that are stored on the [redacted].

Retention

[36] Retention is an important consideration when determining the security measures that are necessary to protect the personal information while it is stored. Shorter retention periods reduce the risk of a breach.

[37] Retention of video surveillance records are generally, in practice, retained for relatively short periods of time. The measure of an appropriate retention period as it pertains to the VST Records will be as determined by the Department to meet the purpose of its collection of this information.

[38] There is a requirement in the ATIPPA for the Department to retain personal information for one year if the information is used to make a decision that directly affect the individual. The VS Policy identifies this requirement. As such, I have no further comments about this requirement.

[39] There appears to be no consistency in the retention of the personal information in the VST records that are not subject to the one-year retention rule. The documents provided indicate five different retention periods identified in relation to the VST Records. The answers provided by the schools surveyed by the Department in relation to the investigation identifies that some VST Records are retained for seven days or 14 days. The PIAs provided[30] indicate 30 days and four weeks respectively. The VS Policy requires the VST Records to be deleted within 45 calendar days.

[40] The PIAs fails to answer the question regarding the existence of a records retention schedule. The document package does contain a document named “records series description

[30] PIAs were provided for the use of VST at [redacted] dated Jan/21 (unsigned) and [redacted], dated Aug 3/20 (unsigned).

summary"[31] but it is incomplete, not dated, not signed and does not explain what the purpose of the document is, nor does it address records retention.

[41] The Department should specify in the VS Policy exactly how long the VST Records should be retained. Having one time period for retention will eliminate any confusion about accessibility and destruction and provide clarity for the right of access to information by persons under the ATIPPA.

Destruction

[42] No procedure or standards regarding the secure destruction were provided by the Department. The YG Corporate Security Policy mentioned is not included in the list of policies identified in the PIA and may not exist. The author of the PIA may either mean the Information Security Management Plan or the GAM 2.15. Neither of these have been provided.

[43] The VS Policy does not need to specify how destruction of the VST Records will occur to ensure that a secure method of destruction occurs. The Department should, however, incorporate into any information management practices that it has how this will occur, noting that these practices must be in writing.

Access Controls

[44] The VS Policy identifies who has access to the VST Records. [redacted].[32]

[45] It also requires that a log be kept of any access to the VST Records and requires that a reason be given for reviewing the information in the VST Records as well as the identity of the reviewer must be logged. It also requires that the building administrator keep a copy of the log and forward a copy to the Assistant Deputy Minister of Public Schools.

[46] The VS Policy is silent on how access is granted, by whom and how it is controlled.

[31] See Department of Education, *records series description summary.* No date.
[32] VS Policy, at p. 5.

[47] Both PIAs indicate that access will be controlled and documented through the "system access security measures". Neither of the PIAs elaborate on what these measures are, and no documentation or other evidence was provided to support that these measures exist.[33]

[48] In practice, some of the schools do not keep access logs as required by ATIPPA and the VS Policy.[34] For some of the logs that are kept, they do not meet the VS Policy requirement: "…must include a record of the reason for the review of video surveillance information, as well as the persons conducting the review".[35]

[49] This gap should be rectified by incorporating the rules for access into the VS Policy, including who is responsible for managing any access to the VST Records and rules to ensure that access is adequately controlled through documented processes that track when access is granted, by whom, to whom, when, for what purpose, and when access is removed.

[50] It should also be included in the VS Policy that the principal or some other person designated in the policy by title, be responsible for ensuring that the access logs are being completed as required by the VS Policy.

Breach Reporting and Management

[51] Although the Department indicated that it has privacy breach reporting policy, this document was not provided as part of the document packages. Both PIAs reference a Department privacy breach policy.

[52] Because access control, logging and auditing are deficient, breaches of personal information may go undetected.

[53] The VS Policy is silent on breach reporting and management. Internal breach reporting is mandatory in the ATIPPA for any unauthorized use of personal information (sections 20) or unauthorized disclosure of personal information (section 24). Notification about a breach to an affected individual and the IPC is mandatory where there is a risk of significant harm to an individual as a result of the breach. Given these new requirements, the VS Policy should include a requirement to report breaches of the personal information in the VST Records as soon as they are discovered, and the VS Policy should specify to whom breaches are to be reported to. The VS

[33] [redacted] PIA, at p. 13, and [redacted] PIA, at p. 12.
[34] See Appendix A.
[35] See e.g., [redacted] log i.e., record re person conducting review is not made. Also, the reason for review is sometimes not clear [redacted] uses a template that does meet these requirements.

Policy should also include a link to the Department's privacy breach policy for quick reference should a breach occur.

Conclusion - Policy, procedures, and practices

[54] For the foregoing reasons, I am of the view that the Department is not fully meeting its obligations under Section 30 of the ATIPPA and section 9 of the Regulation as it relates to its duties thereunder to have in place adequate policies, procedures and practices to protect the VST Records, which must also be in writing.

Observation Regarding Notice

[55] Because the Department is directly collecting the personal information in the VST Records from individuals via VST, it is obligated to provide notice in accordance with subsection 17 (1) and (2) of the ATIPPA.

[56] In the documents provided, there are sample notices that are included in the VS Policy and copies of notices that are being used by the seven schools. On the matter of notice, the Department included the following in its submissions for the investigation.

> *"Response: All schools utilizing video surveillance display public notification of the use of Video Surveillance and collection of personal information, in accordance with section 17 of the ATIPPA, at the entrance to each school. A number of schools have additional notices posted, but none have notices posted at all areas being recorded within the school. According to the Video Surveillance policy, students, parents, staff and the public are to be notified annually that video surveillance is being used to collect personal information. It is not apparent at this time that all schools are sending these notices home to students at the start of each school year."*

Relevant law

[57] As indicated, the requirements for notice are set out in subsection 17 (1) and (2) of the ATIPPA. They are as follows.

"17(1) Subject to subsection (3),[36] a public body that collects personal information directly from an individual must provide a notice to the individual in accordance with subsection (2).

(2) A notice to an individual under subsection (1) must specify

(a) the purpose of the collection of their personal information;

(b) the business contact information of the employee of the public body who is responsible for answering the individual's questions about the collection; and

(c) the public body's legal authority for the collection."

Analysis - Notice

[58] The requirement to provide notice under subsections 17 (1) and (2) does not specify when the notice must be given. However, in the context of video surveillance, it is a best practice to provide individuals with notice prior to their entering the area under video surveillance to give them the option not to have their personal information recorded. To facilitate this choice, notice about the collection of personal information by video surveillance should be placed in an area most likely to be seen by individuals prior to entering the area under video surveillance. As well, notices posted should be understandable and written in simple language and it should be clear from the notice what area is under video surveillance.

[59] The Department's Policy regarding notice reads:

"The Department of Education will ensure that students, parents, staff and the public are notified annually that video surveillance is being used…"

and

"The Department of Education will further ensure that students, staff and members of the public have reasonable and adequate warning that surveillance is, or may be, in operation by using clearly written signs, prominently displayed at the perimeter [37] of the video security surveillance area, identifying video surveillance equipment locations."

[36] Subsection (3) authorizes a public body to not provide notice in certain circumstances. The Department has provided no information to indicate that any of those circumstances apply to the collection of personal information by the Department using VST.
[37] Underline mine.

[60] As indicated, the Department's submission states that:

> *"…All schools utilizing video surveillance display public notification of the use of Video Surveillance and collection of personal information, in accordance with section 17 of the ATIPPA,…"*

[61] The supporting document package lists various photographs of signs used by the schools to notify about active use of VST.[38] Some signs are or include the notice as included in the VS Policy at Appendix 2.

[62] Some signs appear to be supplied by vendors of VST. These sign state only that video surveillance is active. Locations of signs vary per school. Some schools have signs in the schools and some on perimeter fences and posts as well. As per the Departments submission;

> *… A number of schools have additional notices posted, but none have notices posted at all areas being recorded within the school.*

[63] Some schools provide a one-time or yearly recuring notice about VST being used to parents. Some schools assert that they do not provide this yearly notice. Others did not provide the yearly notice but are now providing this notice as a result of the inquiry prompted by my investigation. For this analysis I am relying on the written responses regarding this subject from school administrators. No date stamped evidence regarding yearly sent notices was provided.[39]

[64] A mix of notices are being used by the various schools. Some contain most of the information required except that they need to be updated to reflect the provisions of the new ATIPPA. Other notices are non-compliant because they consist of only a pictogram with some minimal wording (e.g., camera's active, premise under video surveillance, etc.).

[65] It is not clear from the supplied documents if all signs at some of the schools have been reported. Just one school[40] self reported and provided some evidence that they may have sufficient signage to meet the standard as per the VS Policy. However, this has not been verified to my satisfaction as there is no map provided of the locations of the signage.

[66] Neither the template notice in the VS Policy, nor the posted notices in the schools have been updated to reflect the new ATIPPA.

---

[38] See Appendix A for details.

[39] *Ibid.*

[40] [redacted] reports having notices at their main entrances and at some locations exterior to the school. See appendix A for more details.

[67] The yearly notice is not given consistently across all schools that deploy VST.[41]

Conclusion - Notice

[68] For the following reasons, my observation is that the Department does not ensure that adequate notice is provided in the schools that use VST as required by the ATIPPA and in accordance with best practices concerning notice about the use of VST.

1. Several schools are not providing the annual notice as per the VS Policy. The Department is aware of this fact as per the submissions it provided.

2. In most locations that are subject to VST there is not adequate notice. Although all schools provide some form of notice via signage, these signs are not present for each camera or area under surveillance. In addition, no evidence been provided to support that a person who enters an area that is under surveillance could reasonably see a notice (e.g., for the use of VST inside a school, each entrance has a visible and compliant notice, the crux being that one is aware surveillance takes place before one decides to enter the area). The Department confirms in its submissions regarding notices in the schools that:

   "none have notices posted at all areas being recorded within the school"

3. The notices are not uniform or up to date. Notices should be as per the VS Policy and should be updated to reflect the new ATIPPA. The notices should be accompanied by a map that flags where the cameras are located and how they are aimed to ensure that anyone who enters these areas knows the extent of the surveillance taking place.

[69] If the purpose of using VST is to deter violence or other crime, notice is an integral part of achieving that objective.

Security

[70] The following issues will be examined to determine compliance with the security requirements under the ATIPPA.

1. Who has access to the personal information and why?

[41] See appendix A.

2. What technical, administrative, and physical controls that assure confidentiality, integrity, and availability in each step of the lifecycle are in place?

[71] As indicated, the Department made no submissions for the purpose of the compliance audit but did include some relevant documents in its submissions package.

Relevant law

[72] The same Security Measures identified above are applicable to these issues.

Access

[73] In the survey conducted by the Department of schools use of VST in relation to the investigation, some schools indicated that persons other than the building administrator and designated Department employee have access to the VST Records, specifically vendors of VST and ICT personnel.

[74] As for the vendors, it is unclear from the evidence if any vendors have access to the VST Records when maintaining the systems.[42] No agreement regarding the maintenance has been provided or included with the PIAs.

[75] It is unclear from the evidence if ICT personnel have access to the VST Records as part of their administration of systems duties for Yukon government systems. No agreement regarding the services provided by ICT was provided as part of the document package.

[76] It is also unclear from the evidence, if the VST Records are stored on a separate drive that is access controlled.

[77] No proof of authorized access has been provided for any person who has access i.e., description or delegation of authority to access and/or manage the records. It is unclear from the evidence how many individuals access the VST Records in practice.

[78] It is also unclear from the evidence how and when revocation of access to the VST Records takes place (i.e., withdrawal of authority and adjustment of controls such as the return of keys to the video surveillance room or revocation of VST system account access rights).

[42] [redacted] PIA page 12.

[79] The PIAs indicate that the "[s]ystem will have an audit log that can track user ID, date and time video data is viewed".[43] Logging and auditing access to the VST Records is necessary to deter and detect unauthorized access.

[80] If the Department recommences use of VST in any of the seven schools, it should, prior to resuming its use:

1. identify all persons, including vendors of VST, ICT personnel and other contractors, who can access the VST Records and ensure the access is authorized in accordance with ATIPPA, which may require the Department to enter into service provider or information manager agreements (as applicable);

2. ensure that the VST Records are stored on a separate drive that is dedicated solely for the purposes of storing the VST Records and that is access controlled, or if stored on a drive that is accessible by others for work related purposes, that the video surveillance program database is access controlled;

3. ensure that any access to the VST Records, regardless of where they are stored, is logged and audited on a periodic and random basis and that any person with access to the VST Records is informed about the logging and auditing procedures as a measure to deter unauthorized access, noting that these procedures must be in writing; and

4. ensure the VS Policy is updated to incorporate the rules that I identified in paragraphs [49] and [50] of this compliance audit report regarding access and that these rules are implemented.

Controls that assure confidentiality, integrity, and availability

[81] The ATIPPA, lists the Security Measures as minimum controls that are necessary to protect confidentiality, availability and integrity of the VST records. I have already addressed issues identified concerning the gaps in VS Policy, practice and procedure as it relates to this duty. As such, my comments for this issue will focus on the security of the VST Records' storage device.

[82] [redacted].

[43] [redacted] PIA, at p. 14, and [redacted] PIA, at p. 12.

[83] The VS Policy requires that the device on which the VST Records are stored to be "password protected, encrypted and stored in a secure area." The definition of 'storage device' in the VS Policy identifies things on which data can be stored, including a videotape, computer disk or drive, CD-ROM, computer chip. The list is non-exhaustive as it includes "other device used to store the recorded data…captured by a video surveillance system".

[84] "Device" is not defined the VS Policy. Its ordinary meaning will suffice.

> *A thing made or adapted for a particular purpose, especially a piece of mechanical or electronic equipment.*[44]

[85] [redacted]

[86] No evidence has been provided that the storage devices are encrypted as is required by the VS Policy. The PIAs only mention encryption of passwords and flag unencrypted transmission of video footage.[45] In addition, there is insufficient evidence to determine if [redacted]

[87] Paper usage logs, as opposed to those generated by the VST system, do not meet the standards as set out by the Policy as either they do not exist or mostly miss elements such as "the persons conducting the review" or a clear description of "reason for the review".[46]

[88] The PIAs state further that:[47]

> *"The program can identify who (or whose password), when, and where (what computer) information has been accessed. Software can also determine if personal information was saved (video/image data), and downloaded for unintended use. System will have an audit log that can track user ID, date and time video data is viewed. "*

[89] It is unclear if password or account sharing takes place as this seems to be implied when the writer of the PIA states that "the program can identify … who's password" has been used to access the VST Records. This implies that access logging does not meet the requirements of the Regulation. Multiple users using the same user/password negates the non-repudiation that makes

[44] Online Oxford Dictionary: https://www.lexico.com/definition/device.
[45] [redacted] PIA, at p. 12.
[46] See appendix A for an overview regarding log keeping practices by the schools.
[47] [redacted] PIA page 14, [redacted] PIA page 12.

logs useful for investigations and audits. If passwords or accounts are shared and used by more than one individual, this practice must stop.

[90] Furthermore, the references to "can identify" and "will have an audit log that can track" in the PIAs are concerning. [48] The ability to create a system log and the ability to audit does not equal the practice of effective auditing. No active use of auditing capabilities or existence of audit practices has been reported. Without effective auditing, logging is not an effective control.

[91] One of the PIAs also states that:[49]

> *"an authorized user can access the data wherever there is a computer with internet access"*

[92] Without a proper (standardized, tested and active) logging and auditing practice in place, this greatly increases the risk of unauthorized use (snooping) and unauthorized disclosure.

Conclusion - Security

[93] The Department has not supplied sufficient evidence to demonstrate that it is adequately protecting the VS Records from unauthorized access. It has also not provided sufficient evidence to support that it is adequately protecting the confidentiality, integrity and availability of the personal information in the VS Records throughout its lifecycle for the following reasons:

1. there is no evidence that the storage devices on which the VS Records reside are encrypted as required by the VS Policy;
2. the risk of unauthorized access or disclosure and snooping due to a failure to adequately manage, log and audit access; and
3. the failure to provide evidence about the physical security in place to protect the storage device and the VS Records stored therein.

Recommendations

[94] In order meet its obligations under the ATIPPA and Regulation mentioned herein, I recommend that the Department:

Policy, procedure and practices

[48] [redacted] PIA, s.3.7.4, at p. 12 and [redacted] PIA, s.3.73, at p. 12.
[49] [redacted] PIA page 15.

1. update the VS Policy to meet the requirements in the ATIPPA and the Regulation;

Collection, use and disclosure

2. define in the VS Policy the meaning of 'collection', 'use' and 'disclosure' of the personal information in the VST Records as per the meaning of these terms in the ATIPPA;

3. incorporate the rules for collection of personal information as a result of using VST in a school into the VS Policy;

4. clarify in the VS policy that:

   (a) the personal information in the VST Records may ***only*** be used or disclosed for the purpose of addressing significant and serious incidents that threaten the health or safety of students in the school or for addressing significant and serious damage to school property or as otherwise authorized under section 21 regarding use and section 25 regarding disclosure;

   (b) the amount of personal information that may be used or disclosed for the purpose identified in recommendation 4 (a) is that which is reasonably necessary to enable the Department to carry out the Activity to which the use relates or to carry out the purpose of disclosure, as applicable; and

   (c) if consent is relied on to use or disclose the personal information, the consent must be in accordance with the requirements in the Regulation;

5. provide some examples in the VS Policy of what constitutes significant and serious incidents that threaten the health or safety of students in the school or significant and serious damage to school property and what does not to assist those employees who have access to the VST Records determine when it is appropriate to use or disclose the personal information in the VST Records;

6. clarify in the VS Policy that any unauthorized use or disclosure of the personal information in the VST Records is a reportable breach and may qualify as an offence;

7. set out in the VS Policy any routine disclosures, the authority for these disclosures, and that no personal information in the VST records may be disclosed, no matter the circumstances, unless authorized by the ATIPPA;

8. require in the VS Policy that permission be sought for any non-routine disclosures of personal information from a designated individual in the VS Policy who is identified as responsible for making these determinations;

9. identify in the VS Policy the contact information for the designated individual in the Department who is responsible for determining whether a use or disclosure of personal information in a VST Record is authorized;

Secure storage

10. ensure that the storage device on which the VST Records are stored:

    (a) is access controlled such that no person has access to the VST Records unless expressly permitted in accordance with the Department's written procedure on granting, managing and removing access to the VST Records;

    (b) is secure by implementing adequate controls, such as through the use of locks or other forms of physical access control, encryption, management of service providers' access through agreements that ensure the compliance with the ATIPPA;

11. develop and implement written information security policies and practices that are adequate to protect the VST Records that are stored on the storage device;

12. satisfy itself that the network operated by ICT is adequately secured against unauthorized access to the VST Records by any person whether internal or external to the Department;

Retention and secure destruction

13. in addition to the one-year retention rule in the ATIPPA, specify in the VS Policy the specific number of days that the VST Records should be retained;

14. include the retention of the VST Records in its records retention documents;

15. incorporate into its information management practices a procedure for ensuring secure destruction of the VST Records;

Access controls

16. incorporate into the VS Policy

(a) the rules for accessing the VST Records including who is responsible for managing any access and rules to ensure that access is adequately controlled through documented processes that track when access is granted, by whom, to whom, when, for what purpose, and when access is removed; and

(b) that the principal or some other person who is designated in the policy by title, is responsible for ensuring that the paper access logs are being completed as required by the VS Policy and for protecting the confidentiality, integrity and availability of the logs;

Breach reporting

(c) include in the VS Policy a requirement to report privacy breaches of the personal information in the VST Records as soon as they are discovered and to whom (identified by title in the VS Policy) the breaches are to be reported to; and

(d) include a link to the Department's breach policy for quick reference should a breach occur;

Completion of PIAs

(e) identify a person in the Department responsible for ensuring that a PIA is completed and approved by the appropriate Department personnel for any planned use of VST in a school prior to deployment of the VST and include the title of this person in the VS Policy;

Notice

17. ensure that notice is provided by making it publicly viewable by any person prior to their entering a location that uses VST;

18. ensure the notices meet the requirements of subsections 17 (1) and (2) of the ATIPPA;

19. ensure notices are written in simple language and specifies the area under video surveillance;

20. determine how to effectively give notice to students who may not be able to read; and

21. revises the VS Policy by incorporating the requirements in recommendations 17 to 20;

Security

22. prior to deploying VST in any school:

(a) identify all persons, including vendors of VST, ICT personnel and other contractors, who require access to the VST Records to do their jobs or to provide their services, as applicable;

(b) ensure that any access to the VST Records by a vendor is limited to necessary vendor-related purposes and specifies, in addition to any other requirements in the ATIPPA that may be applicable, that the personal information is under the control of the Department and requires that the vendor adhere to the Department's privacy and security policies and practices as it relates to this personal information;

(c) ensure that the VST Records are stored on a separate drive that is dedicated solely for the purposes of storing the VST Records and that is access controlled, or if stored on a drive that is accessible by others for work related purposes, that the video surveillance program database is access controlled; and

(d) ensure that any access to the VST Records, regardless of where they are stored, is logged and audited on a periodic and random basis and that any person with access to the VST Records is informed about the logging and auditing procedures, which must be in writing; and

(e) ensure that password or account sharing is not occurring;

(f) incorporate into the VS Policy a requirement that the logs (electronic or paper) are periodically and randomly audited for the purpose of detecting unauthorized access, such as snooping, use or disclosure of the personal information in the VS Records;

(g) create and implement requirements to ensure the personal information in the VST records is secure against unauthorized access, disclosure or loss and that the integrity and availability of the information is maintained until the records are securely destroyed following ATIPPA compliant and standardized rules and procedures around retention;

(h) deploy encryption of the VST records when in transit and at when at rest;

(i) ensure all access to the VST records is logged and that the logs are retained for at least the same amount of time as the VST Records associated with the logs are retained;

(j) ensure that there is auditing of the access to the VST records;[50] and

(k) ensure that persons who access the VST records are provided their own credential for access and that these credentials are not shared with others;

23. if the Department accepts recommendations 1 to 22 herein, I recommend that prior to deploying VST in any Yukon school, that it demonstrate to the IPC that it has implemented these recommendations by providing me with its revised VS Policy and any other related policies and procedures or other documentation; and

24. the Department inform me within **15 business days** of receiving this Compliance Audit Report about whether it will accept recommendations 1 to 23.

[redacted]

Diane McLeod-McKay
Information and Privacy Commissioner

Distribution List: Head of the Public Body

Attachments: Appendix A

[50] See the OIPC's guidance regarding logging and auditing for guidance in achieving this https://www.yukonombudsman.ca/yukon-information-and-privacy-commissioner/for-public-bodies/resources