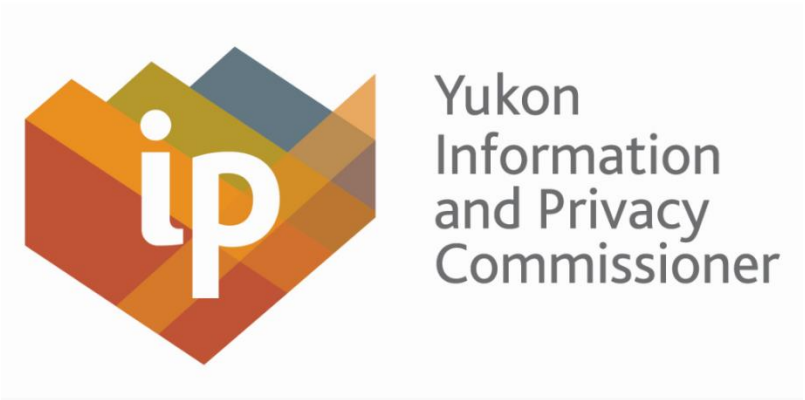


PRIVACY COMPLIANCE AUDIT

Pursuant to Subsection 111(1) of the

Access to Information and Protection of Privacy Act

Department of Education
File ATP-CMP-2023-01-071

Tara Martin, Director
Office of the Information and Privacy Commissioner
May 18, 2023

Summary

Some Yukon Public schools are collecting, using and disclosing student images and videos on internet platforms, including social media, as part of their outreach with parents and the community.

The Information and Privacy Commissioner conducted a compliance audit and found the following.

The Department did not establish that it has authority to collect, use or disclose students' personal information for the purpose of posting it to internet platforms, nor did it establish that it is complying with the limitation principles outlined in sections 12, 19 and 23.

The Department did not demonstrate that it is protecting students' personal information in accordance with its obligations under ATIPPA section 30 and *Regulation* section 9.

Some Department employees are using their work contact information to create social media pages. As such, they may be collecting, using and disclosing students' personal information without authority under the *ATIPPA* and contrary to the Department's policies and procedures.

The Department does not currently have a department-specific 'privacy breach protocol' or a 'privacy management program' that is sufficient to meet the requirements of the ATIPPA and the *Regulation*.

As such, the Information and Privacy Commissioner made six recommendations to remedy these issues.

Table of Contents

Jurisdiction

The IPC's authority to conduct compliance audits is set out as follows.

> *111(1) In addition to the Commissioner's other powers under this Act, the Commissioner may…*
>
> *(b) conduct, in accordance with subsection (2) and the regulations, if any, a privacy compliance audit of a public body for the purpose of assessing the public body's exercise of a power, or performance of a duty, under a provision of Part 2, including*
>
> *(i) the public body's provision of a personal identity service, or*
>
> *(ii) the public body's management of the personal information that it holds;*

Statutes and Regulations Cited

Access to Information and Protection of Privacy Act, SY 2018, c.9

Access to Information and Protection of Privacy Regulation, OIC 2021/025

Education Act, RSY 2002, c.61

Documents

Parental Release of Student Images and Work – currently in use

Updated Release of Student Images form – currently under revision

Web Publishing Guidelines for Yukon Schools

Fact Sheet on Good Practices for School Websites

Statement of School Website Responsibilities

YESNet School Website Guidelines

Social Media Guidelines One Pager

Social Media Account Application form

Student Enrolment form

Privacy Compliance Audit School Inventory, Jan 2023 – excel spreadsheet provided by the Department of Education

Explanatory Note

All section references in this report (Report) are to the *Access to Information and Protection of Privacy Act* (ATIPPA), unless otherwise stated.

Images of students, including photos, video and sound, constitute their personal information as defined under the ATIPPA.

The collection of student personal information (*e.g.,* photos, video, sound, etc.) by the Department of Education (Department) constitutes a 'direct collection' of personal information as defined under the ATIPPA.

Parents/caregivers/guardians generally have the right to make decisions regarding the collection, use and disclosure of their minor children's personal information in accordance with section 118(e).

'Internet Platforms' means any medium whereby content (including, but not limited to images, videos, messages and sound files) is broadcast to, or capable of being broadcast to, the general public or a significant section of the general public. For clarity, and by way of example, Internet Platforms include but are not limited to school webpages, YouTube, Facebook, Instagram, Twitter and also any 'blog' or other type of web journal.

Introduction

[1] The Information and Privacy Commissioner (IPC) became aware that some Yukon Public schools are collecting, using and disclosing student images and videos on internet platforms, including social media, as part of their outreach with parents and the community.

[2] Public bodies must have authority under the ATIPPA and the *Access to Information and Protection of Privacy Regulation* [O.I.C. 2021/025] (*Regulation*) to collect, use and disclose personal information. As well, public bodies are obligated to adequately secure personal information in its custody or control The Department of Education (Department) is a public body that is subject to the ATIPPA.

[3] Given the sensitive and personal nature of the images and videos of children and youth going about their daily activities in school, and considering the possible privacy risks associated with using internet platforms and social media, the IPC felt that it was appropriate to examine

the Department's policies, procedures, practices, and information security. On January 27, 2023, the IPC launched a privacy compliance audit (Compliance Audit) to assess the Department's use of student personal information on internet platforms. The IPC then assigned me as the auditor.

[4] Through this process, I endeavored to understand which schools were using internet platforms for sharing videos and images of students and staff, as well as which platforms were being used. I also wanted to assess whether the Department was meeting its requirements under the ATIPPA with respect to the collection, use and disclosure of personal information, as well as meeting its obligations for managing and securing the personal information.

[5] As such, I identified the following areas of non-compliance.

- The Department has not established that it has authority to collect, use or disclose students' personal information for the purpose of posting it to internet platforms. In addition, the Department has not established that it is complying with the limitation principles outlined in sections 12, 19 and 23.
- The Department has not demonstrated that it is protecting students' personal information in accordance with its obligations under ATIPPA section 30 and *Regulation* section 9, including adequate administrative policies, procedures, and securing the information at all stages of its lifecycle.
- It appears that employees of the Department are using their work contact information to create and maintain social media pages. They may also be collecting, using and disclosing students' personal information without authority under the ATIPPA, as well as contrary to the Department's current policies and procedures.
- The Department does not currently have a department-specific 'Privacy Breach Protocol' or a 'Privacy Management Program' that is sufficient to meet the requirements of the ATIPPA and the *Regulation*.

[6] Each of these areas of non-compliance are discussed in more detail below and include my recommendations.

Background

[7] On January 27, 2023, the IPC issued a Notice to Produce Records (NTPR) to the Department.

[8] On February 13, 2023, I received the Department's response to the NTPR including the Department's policies, procedures, forms and guidance documents relating to the use of

internet platforms by Yukon public schools, as well as the management of students' personal information for the purposes of using it on social media platforms or for posting on a school's internet web page. After an initial review of the documentation provided, I engaged with the Department through email to further clarify specific details.

[9] The conclusions, recommendations and observations of this Compliance Audit are based on the information provided in the Department's response to the NTPR, including subsequent exchanges.

[10] I provided a draft of this Report to the Department for comments on April 6, 2023. It replied on April 28. Some of its comments with respect to its authority to collect, use and disclose student personal information are identified in this Report.

[11] The IPC may exercise its discretion to conduct additional compliance audits in the future, as they see fit.

Issues

1) Does the department have the authority to collect, use or disclose students' personal information for the purpose of posting it to internet platforms and is it complying with the limitation principles outlined in sections 12, 19 and 23?

2) Are Department employees using their work contact information to create social media pages? If yes, then are they collecting, using and disclosing students' personal information without authority under the ATIPPA and contrary to the Department's policies and procedures?

3) Does the Department have a department-specific 'privacy breach protocol' or a 'privacy management program' that is sufficient to meet the requirements of the ATIPPA and the *Regulation*?

Collection – Section 15

[12] To meet the threshold for directly collecting personal information, a public body must clearly establish which ATIPPA section(s) it is relying on.

[13] The Department confirmed that it is relying on paragraph 15(d) to collect students' personal information. This provision states as follows.

15 A public body may collect the personal information of an individual only if …

(d) the collection is for a prescribed purpose other than a purpose referred to in paragraphs (a) to (c) and the individual consents, in the prescribed manner, to that collection.

[14] Paragraph 125(1)(e) allows the Commissioner in Executive Council to make regulations prescribing a purpose under paragraph 15(d). There are no prescribed purposes in the *Regulation* nor in any other ATIPPA regulation. As such, I find that the Department cannot rely on paragraph 15(d) to collect students' personal information for the purpose of posting it on internet platforms.

[15] In the absence of a regulation outlining a prescribed purpose under paragraph 15(d), the Department can only rely on paragraphs 15(a) through (c) to collect personal information. The Department has not established its authority to collect the personal information at issue under these provisions.

[16] It follows that if the Department does not have the authority to collect students' personal information, then it does not have authority to use or disclose this personal information for the purpose of posting it to internet platforms.

[17] Additionally, the Department has not established how it is meeting the limitation principles set out in sections 12, 19 and 23. These provisions stipulate that public bodies must only collect, use or disclosure the minimum amount of personal information that is necessary to carry out their stated purpose.

Note: *In its response to the draft Report, the Department acknowledged that its authority to collect students' personal information is not found in paragraph 15(d); rather, it is provided by subparagraph 15(c)(i). It also stated that paragraphs 21(a) and (b) provide its authority to use this personal information and that paragraph 25(a) provides its authority to disclose this personal information.*

This information was provided to me after I completed the Compliance Audit. In addition, the Department did not include any submissions as to why it had decided to rely on these provisions. As such, I make no comments or findings on the Department's response.

Other ATIPPA Requirements

[18] Although I have found that the Department does not have authority to collect students' personal information for the purpose of posting to internet platforms, I note that it has collected this information for many years. Therefore, I have identified other areas of Department non-compliance with the ATIPPA, as outlined below.

Notice Requirements

[19] Section 17 requires public bodies to notify individuals that they are collecting their personal information. The provision states as follows.

> *17(1) Subject to subsection (3), 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.*
>
> *(3)…*
>
> *(4)…*

Parental Release Form

[20] The Department confirmed that it is relying on the 'Parental Release of Student Images and Work' (Parental Release Form) as a 'notice of direct collection' for the collection, use and disclosure of student personal information for the purpose of posting it on internet platforms.

[21] However, a section 17 'notice' is not the same as 'consent'. As previously stated, the Department has not established its authority under paragraphs 15(a) though (c) to collect personal information, nor is there any prescribed collection purpose under paragraph 15(d). Therefore, obtaining parental consent is not sufficient to establish the Department's authority to collect students' personal information.

[22] In addition, the current Parental Release Form is not sufficient to meet the notice requirements of section 17 even if the Department had the requisite collection authority. That said, I acknowledge that the Department has confirmed that the parental release form is currently under revision.

[23] To satisfy the notice requirements under section 17 the Department must satisfy subsections 17(2)(a) through (c).

17 (2)(a)

[24] On review, the Parental Release Form makes no explicit mention that student personal information is being 'collected'. What it does employ are such terms as 'images of your child (photos, videos, sound)' and 'student work'. However, it does not clearly outline that the Department is collecting this information or that this type of information constitutes a child's personal information, all of which is subject to the ATIPPA.

[25] The requirements of paragraph 17(2)(a) are clear. A notice must specify "the purpose of the collection." Because the Parental Release Form makes no mention of collecting a students' personal information, it does not meet the requirements of this provision.

[26] I am also of the view that purpose statement in the Parental Release Form is vague because it does not provide enough information to meaningfully allow a parent to understand that, by providing consent, their child's personal information may be posted on internet platforms, including social media – with its attendant risks. I will discuss these risks later in my analysis.

17(2)(b)

[27] The Parental Release Form includes the following statement:

> *We are collecting your personal information under the following laws: the* Education Act *and the* Access to Information and Protection of Privacy Act*. We use the information on this form to track parental consent to release images of students and their work.* ***If you have any questions about the information you are providing, please contact the Privacy Management Coordinator, Technology and Student Information, 667-8326, toll free 1-800-661-0408 ext. 8326****, Department of Education, 1000 Lewes Blvd., Whitehorse, YT, Y1A 2C6.* [Emphasis mine]

[28] This statement speaks only to the Department's collection of parent/ caregivers/guardian's personal information on the form. As previously noted, it makes no reference to the collection of student personal information.

[29] It is unclear whether the identified contact individual would have been equipped to answer questions about the collection of the parent/caregivers/guardian's information, as well as the collection of student personal information.

[30] For these reasons, the Parental Release Form does not meet requirements of paragraph 17(2)(b).

17(2)(c)

[31] The Parental Release Form contains no mention of the Department's legal authority to collect either a student's or a parent's personal information on the form itself. In addition, it does not cite any specific ATIPPA or *Education Act* provisions.

[32] The statement contained at the bottom of the Parental Release Form only states as follows.

> *We are collecting your personal information under the following laws: the* Education Act *and the* Access to Information and Protection of Privacy Act.

[33] This is not sufficiently detailed to meet the requirements of paragraph 17(2)(c) with respect to the collection of students' personal information.

Revised Parental Release Form

[34] With respect to the 'revised' version of the Parental Release Form provided by the Department for my review, that while many aspects of the form are significantly improved, the same fundamental problem exists. The Department must establish and clearly state its authority under paragraphs 15(a) though (c) to collect students' personal information for the purpose of posting to internet platforms, regardless of parental consent.

Withdrawal of Consent

[35] The Parental Release Form states as follows.

> *You may revoke your consent at any time. This revocation will not be retroactive.*

[36] Even if the Department met the requirements of sections 15(a) through (c) and was able to use this form, there is not an adequate framework within it to manage parental withdrawal of consent, as set out in section 8 of the *Regulation*. In addition, there is no information provided to parents on how they could avail themselves of this process, were it available to them.

Administrative Measures

[37] Section 30 states as follows.

> *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.*

[38] Subsection 9 of the *Regulation*, flowing from section 30 above, states as follows.

> *… 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.*

[39] The requirements for ministerial public bodies include the following administrative measures:

- the establishment of written policies respecting the protection of the personal information it holds;
- ensuring the effectiveness of those policies through periodic testing and evaluation; and
- establishing a written information security strategy regarding the establishment and implementation of security measures and the establishment of policies.

[40] While I acknowledge that the Department has some administrative policies and procedures in place, they are both generic and vague. In the context of this Compliance Audit, they do not contain a sufficient level of detail or specificity to meet the requirements of the ATIPPA. As such, based on the documents and information provided to me, the Department does not have a cohesive framework of administrative policies, procedures, access controls and personal information security in place to manage the collection, use or disclosure of students' personal information being posted on internet platforms.

[41] Some examples of Department non-compliance include the following.

Roles and responsibilities are not clearly defined.

[42] The Department confirmed that the school principal and the administration are responsible for overseeing compliance with respect to students' personal information on internet platforms. However, in practice, only one document called 'Statement of School Website Responsibilities' somewhat outlined these roles. I note that this document is dated 2015 and only relates to school websites and not to social media.

[43] In my view, this administrative security document alone is not an appropriate accountability structure with respect to the collection, use and disclosure of students' personal information.

No mechanisms are in place to ensure compliance with the administrative security policies or procedures, or to evaluate their effectiveness.

[44] According to the Department's own policies, schools seeking to run an 'official' social media page must fill out a 'Social Media Account Application Form'. The Department confirmed that schools with 'official' social media accounts have filled out this form and had their account approved. However, on my request, the Department was unable to provide me with copies of any of the signed and approved application forms.

[45] The Department acknowledged that, once signed (which I was not able to corroborate ever occurred), the form is not typically revisited, reviewed or reconsidered.

[46] I also noted that it is unclear if filling out the form is optional because the following instruction uses the verb 'should' rather than, for example, 'must'.

> *Schools interested in running a social media account should fill out and send this form to the Director of Community Relations and Engagement for discussion and approval by your Area Superintendent.*

[47] The Department confirmed that it intended the Social Media Account Application Form to be mandatory but acknowledged that the language could be clearer.

[48] Overall, I find that there are significant gaps in the Department's management of students' personal information. The policies and procedures relating to internet platforms require significant improvement and must be reconsidered in the context of employing a more comprehensive approach to administrative security. Clear oversight must be established for compliance with these policies and procedures. In addition, they must be updated, reviewed and audited for effectiveness on a regular basis.

Managing Security Breaches

[49] The Department confirmed that it manages all privacy breaches using Yukon Government's (YG) procedures but did not identify them. On review, I must presume that the Department is referring to the Privacy Breach Procedures (December 2021) issued by the ATIPP Office, a branch of the Department of Highways and Public Works. There also exists a toolkit for Designated Privacy Officers (May 2021) within YG that contains more detailed description of the functions and activities assigned to DPOs, as well as more information about privacy breaches.

[50] That said, I am still of the view that the privacy risks associated with posting students' personal information on internet platforms are considerable. Collecting, using and disclosing students' images/videos to internet platforms, particularly social media sites, poses distinct and

serious risks factors with respect to the Department's ability to investigate and mitigate privacy breaches.

[51] Some examples of serious risk factors include the following.

- Data management challenges. These include difficulty in tracking what personal information has been posted to which sites. For a school of several hundred students, keeping track of this information is likely to prove challenging and complex.

- Inability to track or control disseminated personal information. This includes information that is copied or edited. Once it is posted, it may be extremely difficult, if not impossible, to control the unwanted proliferation of student images/videos. This makes it very challenging to manage breaches when they occur.

- No security guarantees. The Department's inability to guarantee that the personal information will not be used for unwanted or unintended purposes, such as the harvesting of personal information by bad actors, cannot be assured.

[52] I note that the Department alludes to these risks in in its 'Social Media guidelines for Yukon Schools' document.

> ***Visitor comments*** – *Schools are responsible for content posted by visitors to their page.* ***Allowing visitors to post on your social media page increases privacy risks because you cannot control the content.*** [Emphasis mine]

[53] However, there is no evidence, based on the information provided to me, that the Department has meaningfully turned its mind to addressing these specific risk factors or notifying parents about them. In my view, this is inconsistent with the ATIPPA principles that impose a binding duty on public bodies to adequately protect and secure personal information in their custody or control.

[54] For these reasons, I find that the Department has not demonstrated that it is protecting students' personal information in accordance with its obligations under ATIPPA section 30 and *Regulation* section 9. This includes insufficient administrative security policies and procedures, as well as the requirement to secure this personal information at all stages of its lifecycle.

Overview of the Department's Use of Internet Platforms

[55] In response to our NTPR, the Department provided our office with an excel spreadsheet containing a list of all Yukon public schools, their website addresses, and their social media pages where applicable.

[56] The Department also stated the following.

> *At this moment, we are not able to definitively say which social media instances are official and maintained by the school* [or] *school council and which may be maintained by a parent or member of the public. We will take the time in the coming weeks to determine this.*

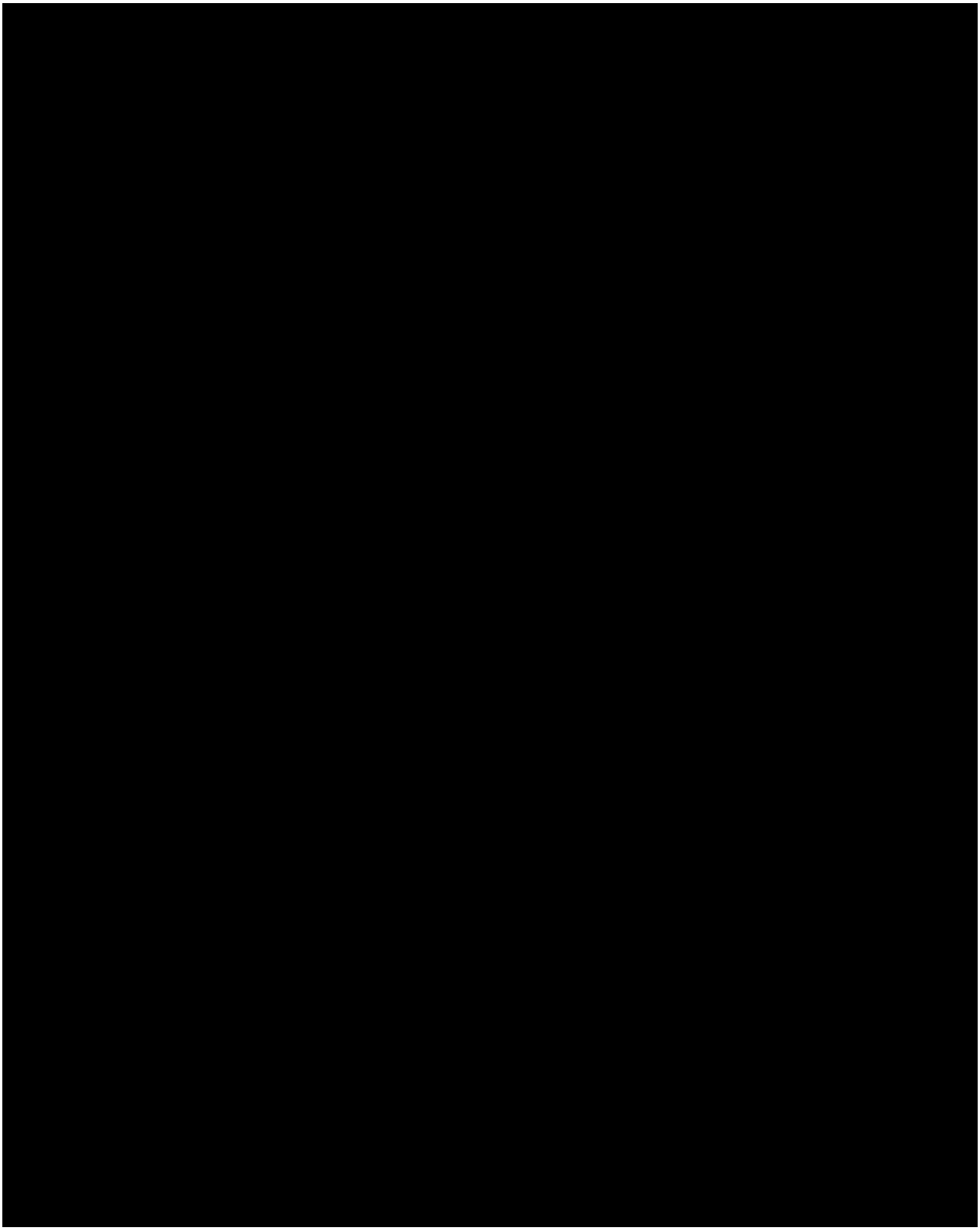
[57] The Department never provided an updated list to me. I therefore relied on the initial list that included the following.

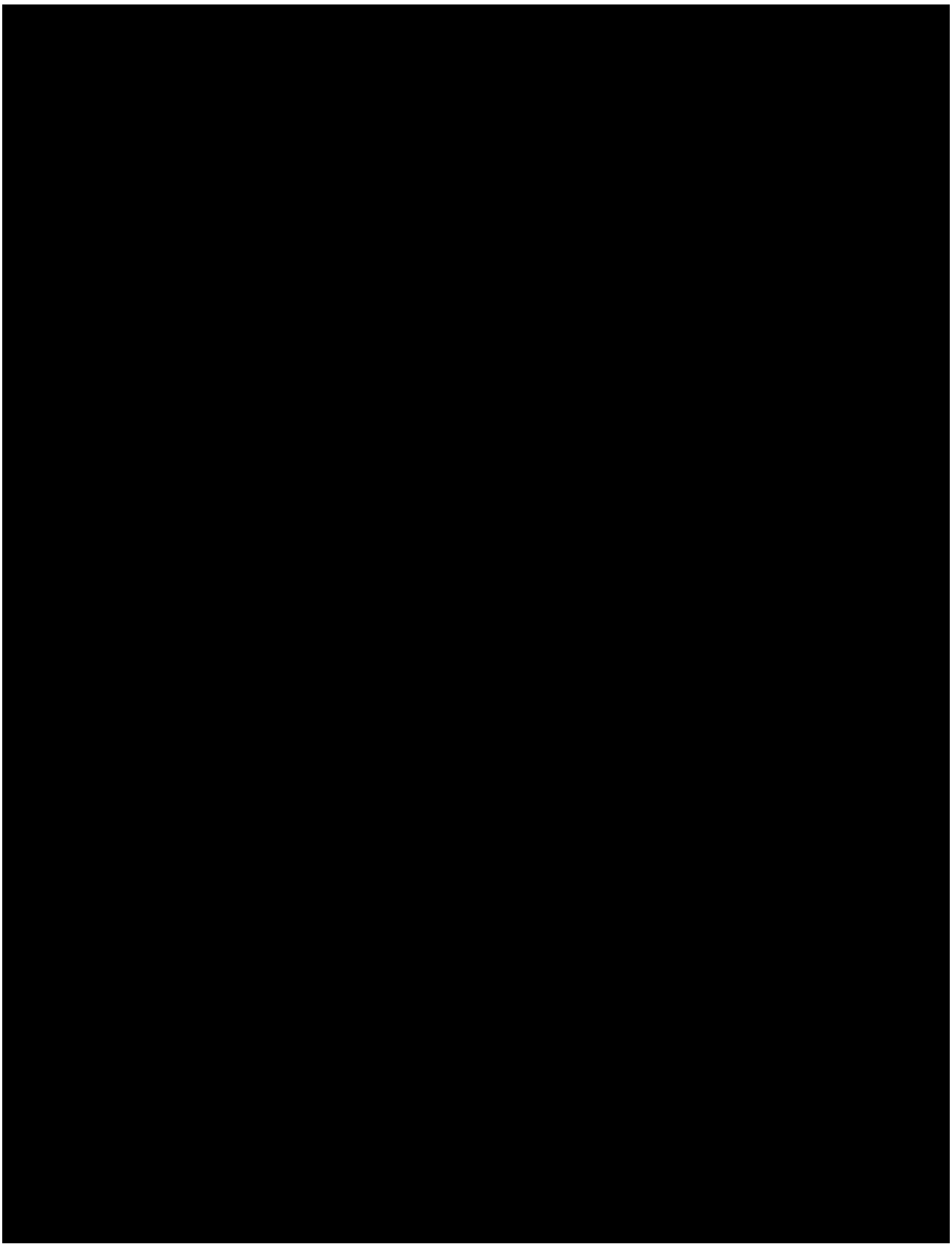
- 4 social media pages were labeled 'OFFICIAL'.
- 13 social media pages were labeled 'UNOFFICIAL'.
- 7 social media pages were labeled 'UNKNOWN'.
- 8 schools had no social media pages.

[58] As part of this Compliance Audit, and to validate the information provided by the Department, I reviewed the first four schools in the spreadsheet having social media pages designated as either 'unofficial' or 'unknown'. In all instances, I found that the contact information associated with the Facebook pages belonged to a Department employee, using their work contact information.

[59] My notes from March 8, 2023, on these findings are set out in the fifth column below.

School Name	School Website	Social Media	Official/ Unofficial	OIPC Comments
[redacted]				





[60] In my view, these findings appear to indicate two possibilities. First, the Department was mistaken in its designation and these social media pages are in fact 'official.' Second, some employees of the Department of Education, using their work contact information, are creating and maintaining school social media pages and may be collecting, using and disclosing student personal information contrary both to the ATIPPA and the Department's own policies and procedures.

[61] If the former is true, then this is further evidence of the Department's lack of appropriate administrative policies and procedures in place to manage the use of internet platforms by Yukon public schools. If the latter is true, then this activity by Department employees may constitute a privacy breach under the ATIPPA.

[62] I did not review any other schools beyond the initial four that I sampled. However, I believe it is reasonable to assume that there may be other examples amongst the remaining 16 schools with 'unknown' or 'unofficial' social media accounts.

[63] For these reasons, I find that some Department employees are using their work contact information to create and maintain social media pages. As such, they may be collecting, using and disclosing students' personal information without any authority under the ATIPPA and contrary to the Department's policies and procedures.

Data Lifecycle Framework for Students' Personal Information on Internet Platforms

[64] In referring again to ATIPPA section 30 and *Regulation* section 9, public bodies must establish and implement administrative, technical and physical security measures to protect the personal information that it holds. Through this Compliance Audit, I confirmed the following.

- The Department does not have written policies or procedures outlining which devices are authorized to collect students' personal information for the purpose of posting to internet platforms.
- The Department does not have written policies or procedures outlining how access controls are managed with respect to internet platforms.
- The Department does not have written policies or procedures outlining how security of the websites and social media accounts are to be managed, such as addressing who can post to the site, who can comment on posts and so forth.
- The Department does not have written policies or procedures ensuring the integrity of students' personal information throughout their lifecycle.

[65] This means that:

- Department employees may be using personal devices to take pictures and videos of students without any oversight.
- Original images/videos are not managed once they are uploaded to internet platforms.
- Images/videos of students may simultaneously exist in multiple places, on multiple devices, with no oversight.
- Images/videos may remain online indefinitely because there is no retention schedule for how long this personal information remains on internet platforms once posted.

[66] For these reasons, I find that the Department has not demonstrated that it is protecting students' personal information in accordance with its obligations under ATIPPA section 30 and *Regulation* section 9.

Conclusions and Recommendations

ISSUE 1

The Department has not established that it has authority to collect, use or disclose students' personal information for the purpose of posting it to internet platforms. The Department also has not established that it is complying with the limitation principles outlined in sections 12, 19 and 23.

Recommendation 1

The Department must immediately cease the collection, use and disclosure of students' personal information on internet platforms until it has clearly established that it has authority under the ATIPPA to do so.

Recommendation 2

The Department must, within a reasonable timeframe, purge all students' personal information from its official internet platforms.

ISSUE 2

The Department has not demonstrated that it is protecting students' personal information in accordance with its obligations under ATIPPA section 30 of the and *Regulation* section 9.

Recommendation 3

If the Department wishes to resume collecting, using and disclosing students' personal information on internet platforms, then it must conduct a 'Privacy Impact Assessment' (PIA) to address and mitigate the associated privacy risks. This work effort must include an assessment of the unique privacy risks associated with internet platforms, as well as meaningfully addressing and mitigating these risks through appropriate policy and procedure.

Pursuant to section 11, the Department may be required to submit a copy of its PIA to our office for review, though our office remains available on request, to provide comments on non-mandatory PIAs.

ISSUE 3

Some Department employees are using their work contact information to create social media pages. As such, they may be collecting, using and disclosing students' personal information without authority under the *ATIPPA* and contrary to the Department's policies and procedures.

Recommendation 4

The Department must undertake a review of all school social media identified in the excel spreadsheet provided to our office to assess for any privacy breaches that may have occurred involving the unauthorized collection, use or disclosure of students' personal information by Department employees.

Recommendation 5

The Department must immediately notify all its employees of their obligations with respect to the collection, use or disclosure of students' personal information under the ATIPPA.

ISSUE 4

The Department does not currently have a department-specific 'privacy breach protocol' or a 'privacy management program' that is sufficient to meet the requirements of the ATIPPA and the *Regulation*, although I acknowledge that this work effort is currently underway and is scheduled for completion this year.

Recommendation 6

If the Department wishes, as part of its current work effort, to resume collecting, using and disclosing students' personal information for the purpose of posting in on internet platforms, then it must address the issues identified in this Privacy Compliance Audit including, but not limited to, the following.

a) Develop and implement an accountability framework that clearly outlines roles, responsibilities and oversight with respect to the collection, use and disclosure of students' personal information on internet platforms.

b) Ensure that the above framework is outlined in *written* policies and procedures.

c) Ensure that the above written policies and procedures are periodically evaluated for effectiveness and audited for compliance.

d) Establish a data management framework that ensures students' personal information is collected, used and disclosed in compliance with the ATIPPA at all stages of the data lifecycle (*i.e.,* collection, use, disclosure, retention, destruction).

Observation

[67] None of the information provided by the Department for this Privacy Compliance Audit addressed the wishes or concerns of the students with respect to the collection, use or disclosure of their personal information for use on internet platforms. While it is the case that parents/caregivers/guardians have the legal authority under the ATIPPA to make decisions with respect to their child's personal information, it is worth noting that their decisions in this respect may not always align with their child's wishes or concerns.

[68] The Department may want to consider conducting a 'Child Rights Impact Assessment' with respect to the collection, use and disclosure of students' personal information on internet platforms. As such, the Department may wish to consider engaging with the Yukon Child and Youth Advocate's Office to assist in this endeavor.

Department Head's Response to our Privacy Compliance Audit

[69] Although not a requirement under ATIPPA, I am providing the Department Head an opportunity to respond to this Privacy Compliance Audit and notify us whether they are accepting or rejecting each recommendation. We ask that you respond within 15 business days from the date of this Report. Please advise me of your decision on or before **June 9, 2023.**

ORIGINAL SIGNED

_____

Tara Martin
Director of Intake and Informal Case Resolution
Office of the Information and Privacy Commissioner

ORIGINAL SIGNED

_____

Jason Pedlar, BA, MA
Information and Privacy Commissioner

Distribution List:

Department Head