



Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 035-2024, 047-2024, 052-2024, 059-2024

Edge Imaging, Living Sky School Division No. 202, Prairie Spirit School Division No. 206, Horizon School Division No. 205

September 18, 2024

Summary:

Edge Imaging notified my office that one of its service providers, Entourage Yearbooks (Entourage), had a cyber incident that may have affected some Saskatchewan School Divisions. Living Sky School Division No. 202, Prairie Spirit School Division No. 206 and Horizon School Division No. 205 also proactively reported a privacy breach to my office regarding this cyber incident. The A/Commissioner found that the notification to affected individuals was not sufficient, as the notifications did not contain all of the necessary elements. The A/Commissioner found that Entourage's investigation identified the root cause of the cyberattack and identified steps that could be taken to prevent future incidents. The A/Commissioner recommended that, in the future, the school divisions ensure their notification contain all the necessary elements when issuing notification to affected individuals. The A/Commissioner also recommended that, going forward, the school divisions ensure they have written agreements with information management service providers (IMSP) in place that address the specific requirements outlined at subsection 23.2(2) of LA FOIP, section 8.2 of *The Local Authority Freedom of Information and Protection of Privacy Regulations* (LA FOIP Regulations) and the key components for a well written agreement and that the school divisions ensure that its policies and procedures clearly sets out the specific requirements in LA FOIP and the LA FOIP Regulations that must be included a written agreement with an IMSP.

I BACKGROUND

[1] On February 15, 2024, Edge Imaging (Edge), a Canadian-owned and operated school photography and yearbook company, notified my office that one of its service providers, Entourage Yearbooks (Entourage), had a cyber incident that may have affected school divisions across Canada. This included some Saskatchewan school divisions that had uploaded photographs (photos) to Entourages' software. Edge's notification to my office provided the following details regarding this matter:

Our company provides photography services to school boards in Saskatchewan, among other jurisdictions.

One of our service providers, Entourage (the owner of the "Creator Studio Pro" yearbook software web platform used by school boards) had a cyber incident on its Canadian Amazon Web Services cloud server that may have affected uploaded images of school boards' students and staff.

...

On February 5, 2024, Entourage recognized a cyber incident on its cloud server due to a compromised username and password of one of its server accounts. The result was a ransomware attack where the threat actor removed photo images on a storage container on that server.

...

We are advised by Entourage that the photos were "raw" and likely contained no other identifying information such as associated names, schools, grades, location, or captions. Entourage recently commented that there may have been some metadata associated with the photos depending on the device from which the photos were uploaded. For instance, it is possible that metadata such as time the photo was taken and location of the photo may have been attached to some photos. The photos span the last 24 months when we first engaged Entourage to support our yearbook services. Edge Imaging's own IT systems were not accessed or affected at all. This incident arises fully from an attack on a vulnerability at Entourage.

[2] On February 20, 2024, Edge clarified that this cyber incident affected 3,505 images uploaded by four schools in Saskatchewan. Edge provided further detail regarding the schools affected by this cyber incident as follows:

School Division	School	2023	2024	Grand Total
Horizon	Muenster School	-	1,099	1,099
Horizon	St. Brieux School	2	2,387	2,389
Living Sky	Kerrobert Composite School	4	-	4
Prairie Spirit	Hepburn School	8	5	13
	Grand Total	14	3,491	3,505

[3] On February 26, 2024, May 9, 2024 and March 4, 2024, respectively, Living Sky School Division No. 202 (Living Sky), Prairie Spirit School Division No. 206 (Prairie Spirit) and Horizon School Division No. 205 (Horizon) proactively reported the incident to my office.

[4] On May 8, 2024, Living Sky provided my office with its completed *Privacy Breach Investigation Questionnaire* (Questionnaire). On May 9, 2024, Prairie Spirit and Horizon each submitted a completed Questionnaire.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction to investigate this matter and is *The Local Authority Freedom of Information and Protection of Privacy Act (LA FOIP)* engaged?

[5] The school divisions are “local authorities” pursuant to subsection 2(1)(f)(viii) of LA FOIP. Therefore, I have jurisdiction to conduct this investigation.

[6] Based on information provided by Edge, school divisions that choose to use Entourage’s software platform upload photos, including images of clubs, events or candid photos. Edge stated that Entourage is the owner of the “Creator Studio Pro yearbook web platform used by school boards, and the uploaded images are then stored on Entourage’s cloud server.” Edge also uploads school photography sessions to the yearbook platform on behalf of the school, if it is the provider. As such, it appears that Edge and Entourage would qualify as “information management service providers” (IMSP) pursuant to subsection 2(1)(e.1) of LA FOIP as follows:

2(1) In this Act:

...

(e.1) “**information management service provider**” means a person who or body that:

(i) processes, stores, archives or destroys records of a local authority containing personal information; or

(ii) provides information management or information technology services to a local authority with respect to records of the local authority containing personal information;

[7] As a privacy breach can only occur if personal information is involved, I next need to consider if personal information is involved.

[8] My office’s *Guide to LA FOIP*, Chapter 6, “Protection of Privacy” (*Guide to LA FOIP*, Ch. 6) at page 39, provides that for the privacy provisions at Part IV of LA FOIP to be engaged, the information at issue must constitute “personal information” as defined by subsection 23(1) of LA FOIP. In order to qualify as personal information, the information must be: 1) about an identifiable individual; and 2) personal in nature.

[9] Pages 39 to 41 of the *Guide to LA FOIP*, Ch. 6, also provides that information is about an “identifiable individual” if the individual can be identified from the information (e.g., their name is provided) or if the information, when combined with information otherwise available, could reasonably allow the individual to be identified. To be “personal in nature” means the information reveals something personal about the identifiable individual.

[10] Living Sky took the position that the information did not qualify as personal information stating as follows:

The breach involved raw images collected and uploaded by Kerrobert Composite School to a third-party platform. No other identifying information such as school, grade, name, or location were affected by the cyber incident. The breach did not involve personal information as defined in section 23 of LA FOIP.

[11] Prairie Spirit's Questionnaire stated as follows:

[Prairie Spirit] understands that 13 yearbook photos from Hepburn School were impacted by this incident.

Following the incident, [Prairie Spirit] began investigating the incident with discussions with Edge Imaging and Entourage. The investigation revealed that the photos were likely candid shots and not specific photos of Hepburn School students or staff, indicating that specific students or staff may not have been impacted. The investigation revealed that the photos contained no other identifying information such as names, schools, grades, location, or captions.

[12] Horizon School's Questionnaire provided the following regarding what personal information data elements were involved and the number of affected individuals:

St. Brieux: ~250,
Muenster: ~190, and

Pictures of individuals without names, but with some associated metadata related to the application, and project ID's.

[13] My office also asked Edge to provide additional clarification about the images involved. Edge stated:

... schools often upload photos of clubs, events or candid photos that are often included in a yearbook...Where we are the school photography provider, we do upload photos from the school photography sessions.

...
Metadata associated with photos taken by Edge Imaging (where Edge is the school photography provider) are limited to date and camera settings; our cameras do not have GPS chips and are not configured to capture geo-location. Photos uploaded directly by schools (e.g. captured by students, teachers, parents) may have had metadata associated with the photos, depending on the camera settings of the individual, however any captions manually added to a photo such as "Child playing trombone" would not be included in the file.

[14] Edge also stated that photos are, "stored in folders that are divided by an algorithm that ties the photo to the user who uploads the photo." Edge further added that users are "mapped to school yearbook projects."

[15] In my office's [Review Report 244-2017](#) concerning the City of Saskatoon, I considered if the release of photos of a dog and its owner who were involved in an incident could allow for the identification of an identifiable individual. In that report, my office referenced the Information and Privacy Commissioner of Ontario (ON IPC) [Order MO-3358](#), which provides as follows:

[36] Previous orders have determined that in order to qualify as “personal information”, the fundamental requirement is that the information must be “about an identifiable individual” and not simply associated with an individual by name or other identifier.

...

[39] ... this office has previously held that information collected about identifiable individuals from video surveillance cameras qualifies as “personal information” under the Act. In that regard, I find that disclosing an individual’s unblurred image on CCTV camera footage... would also **reveal their personal characteristics and that they were present in that place on that date, and their conduct as well as their location and movement at certain times...**

...

[43] ... **individuals may have certain attributes that would result in a reasonable expectation that they could be identifiable** even with the application of blurring technology. A starting point could be section 2(1)(a) of the definition of personal information which provides that personal information includes:

information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual.

[44] Other considerations may also apply. Some orders have considered **a small cell count, where the possibility of identification increases based on the number of possible affected parties. The question then is whether it is reasonable to expect that an individual could be identified because of the size of the group of individuals, the nature of the information at issue, or when the information at issue is combined with information from sources otherwise available.**

[45] Other orders have found that, even if the images are unclear or the faces have been blurred, **there may be something distinctive about an individual that would allow them to be identifiable. It may be that the individual’s attire would set them apart from others on the scene, such as individuals wearing a particular uniform or type of clothing.** It may be that with facial blurring, they remain distinctive and therefore identifiable. Still other order have found that individuals are not identifiable because the images are unclear on the video camera footage or because, in the circumstances the images render the individual unidentifiable.

[Emphasis added]

[16] My office was not provided copies of any of the images involved or details of what metadata, if any, was attached to these images. However, based on factors cited by the ON IPC above, it is likely that some of the images as described by the school divisions and Edge, if not all, could lead to the identification of the individuals on them based on factors such as race, ethnic origin, age, appearance in a certain location, etc. This would then reveal information that is personal in nature about an identifiable individual. Based on this, I find that there is personal information involved.

[17] I also need to consider if the personal information is in the possession or control of the school divisions. My office's *Guide to LA FOIP*, Chapter 1, "Purposes and Scope of LA FOIP" (*Guide to LA FOIP*, Ch. 1) at pages 9 and 10, define possession and control as follows:

- "Possession" is physical possession plus a measure of control over the record.
- "Control" connotes authority. A record is under the control of a local authority when it has the authority to manage the record including restricting, regulating, and administering its use, disclosure, or disposition.

Possession and control are different things. It is conceivable that a local authority might have possession but not control of a record or that it might have control but not possession... If a local authority has either possession or control of a record, LA FOIP applies to that record.

[18] In its notification to my office, Edge stated that Entourage's Canadian Amazon Web Services cloud server was subject to the cyberattack that may have affected images of school division's students and staff who utilized the Creator Studio Pro yearbook software web platform, which Entourage owns. Based on this, it appears that the personal information was not in the possession of the school divisions when the breach occurred, as it was stored on Entourage's web server, but I will consider if the school divisions had control of the personal information.

[19] Edge shared copies of the "Edge Imaging Yearbook Agreement" (Agreement) that it had with each school, with the exception of Horizon's School at Muenster, which did not have a signed Agreement prior to initiating its yearbook project. The Agreement outlines what

appears to be the project deliverables and pricing structure. In the Agreement's footnotes, Edge's "Terms and Conditions" (terms) are referenced. The terms state that Edge "collects essential data that we need to ensure a smooth photo day and delivery of photos." It also states that it securely archives student images, unless requested not to, and stores "data we receive from our customers in order to purchase photos." The terms go on to state that Edge may share personal information with companies it works with so that those companies may provide services (e.g., monetary transaction sites).

[20] The agreement does not reference Entourage's cloud storage server or yearbook web platform, nor does it clearly outline who maintains control of what is uploaded.

[21] In preparing its response to my office's investigation, Living Sky acknowledged that after reviewing the Privacy Policy and terms referenced in the Agreement, that these didn't seem to reference who owns the content once it is uploaded. Living Sky asked Edge to clarify this, and Edge responded as follows:

...the school would be in control of the yearbook project (candid and club photos, captions, layouts, copywriting, etc).

Edge Imaging can assist the school as requested so we also have access to the project...if the school wants it deleted, then they can make sure that happens.

[22] Horizon's response to my office's investigation stated that "we would also expect the information would remain in the control of St. Brieux and Horizon School Division."

[23] None of the school divisions have taken a position that the information would not have been under their control. Based on the information provided by Edge, it appears that the school divisions would (and should) have authority over the images and yearbook project that is stored on Entourage's servers. As such, I find that the school division had control over the personal information.

[24] I add that the school divisions, as the local authorities with control over the personal information, are utilizing Entourage's software and uploading photos to the cloud storage

server. The school divisions have a responsibility to ensure appropriate safeguards are in place when using or disclosing personal information it has in its control. The school divisions cannot contract out of their responsibilities to protect personal information when providing it to an IMSP. The school divisions need to ensure any written agreements they have with such IMSPs include this. I will speak to this further later on in this Investigation Report.

[25] In conclusion, there is personal information involved that was under the control of the school divisions. As the personal information was involved in the cyberattack, I find that a privacy breach occurred. The privacy provisions in Part IV of LA FOIP are then engaged.

2. Has each school division responded to the privacy breach appropriately?

[26] In circumstances where a local authority proactively reports a privacy breach to my office, my office will consider whether the local authority appropriately handled the privacy breach. In order to be satisfied, my office would need to be confident that the local authority took the privacy breach seriously and appropriately addressed it. My office recommends four best practice steps be taken when a local authority discovers a breach of privacy has occurred. These are:

- Contained the breach (as soon as possible)
- Notified affected individuals (as soon as possible)
- Investigated the breach
- Taken steps to prevent future breaches

([Rules of Procedure](#), updated August 2023 at p. 22)

[27] I will consider how the school divisions addressed each of these steps.

Contained the breach (as soon as possible)

[28] The *Guide to LA FOIP*, Ch. 6 at page 236, provides that it is important to contain the breach immediately. In other words, ensure that personal information is no longer at risk. This may involve:

- Stopping the unauthorized practice;
- Recovering the records;
- Shutting down the system that was breached;
- Revoking access to personal health information; and
- Correcting weaknesses in physical security.

[29] In my office's [Investigation Report 197-2022, 215-2022](#), I stated that in assessing an institution's steps to contain the breach, my office applies a reasonableness standard. We want to have some reassurance that the institution has reduced the magnitude of the breach and the risk to affected individuals.

[30] Based on the materials submitted to my office, Entourage's response to the incident outlined the following:

- On February 5, 2024, Entourage's development team recognized an attack on its Canadian Amazon Web Services cloud server. The result was a ransomware attack where the attackers deleted the contents of a number of its storage buckets that were in use. One of these buckets was the photo storage bucket used by the CreatorStudio Application dedicated to Edge. The threat actors then left a message in the emptied storage buckets with instructions that the content of the buckets were downloaded and deleted and they had left emails to contact with instructions on how to pay a ransom for the return of the data.
- Immediate action was taken to secure the application from another attack including, identifying the entry point of the attack, monitoring for further unexpected attacks, daily monitoring of further intrusions (no evidence found of further attacks), access credentials for applications and usernames and passwords for databases updated, reviewed and updated security permissions for all profiles, removed ability for all accounts to delete images and reported the incident the authorities.

[31] Additionally, Edge’s website provided a number of updates on this cyber incident, including an update on February 29, 2024, stating:

The Creator Studio Pro team, working through their cyber security advisors, have reported that they secured the return of all the Canadian photo files from the threat actors, along with their commitment that the photo files have been deleted, and were not distributed.

[32] The following responses were provided by the school divisions regarding containment of the breach:

Prairie Spirit

We did not have direct interactions with the threat actor but was advised that all Hepburn School photos have been recovered and that the threat actor deleted and did not share any Hepburn School photos.

Horizon

I have received responses directly from [Edge’s] CEO... They indicated that the breach was contained, and they were able to restore most if not all of the data. They claimed that they [sic] data was reclaimed, however we have no assurances that the breach was fully contained, and assume that the pictures were captured, and likely still out in the “wild”.

Living Sky

As the breach occurred on the servers of a third-party service, our school division was unable to take direct action to stop the unauthorized practice.

[33] As this breach was cause by a ransomware attack and Entourage is the IMSP, the school divisions have deferred to Entourage for any containment efforts undertaken. Although the cyberattack occurred while the photos were stored on Entourage’s cloud server, the school divisions still retain control of the personal information and have an explicit duty to protect that information under LA FOIP.

[34] Section 23.1 of LA FOIP provides the explicit duty to protect personal information in the possession or under the control of a local authority as follows:

23.1 Subject to the regulations, a local authority shall establish policies and procedures to maintain administrative, technical and physical safeguards that:

(a) protect the integrity, accuracy and confidentiality of the personal information in its possession or under its control;

(b) protect against any reasonably anticipated:

(i) threat or hazard to the security or integrity of the personal information in its possession or under its control;

(ii) loss of the personal information in its possession or under its control; or

(iii) unauthorized access to or use, disclosure or modification of the personal information in its possession or under its control; and

(c) otherwise ensure compliance with this Act by its employees.

[35] Much of the containment efforts fell on Entourage, as an IMSP for the school divisions. The school divisions cannot place all of the fault on the IMSP. Responsibility falls to the school divisions to make certain that its IMSPs are meeting the duty to protect under LA FOIP, as the school divisions still retain control of the information. I will look at this further later in this Investigation Report.

[36] While it appears that steps were taken by Entourage to contain the breach, as noted in my office's [Investigation Report 009-2020, 053-2020, 244-2020](#), there have been cases where stolen data is found for sale on the dark web years later. Given this and the concern that there are no assurances that the breach was fully contained, I find that the breach has not been contained.

Notified affected individuals (as soon as possible)

[37] My office's *Guide to LA FOIP*, Ch. 6 at page 231, explains that section 28.1 of LA FOIP places an obligation on a local authority to notify individuals when their personal information has been breached and a real risk of significant harm exists for the affected individual.

[38] Section 28.1 of LA FOIP states:

28.1 A local authority shall take all reasonable steps to notify an individual of an unauthorized use or disclosure of that individual's personal information by the local authority if it is reasonable in the circumstances to believe that the incident creates a real risk of significant harm to the individual.

[39] Page 232 of the *Guide to LA FOIP*, Ch. 6, emphasizes that even where section 28.1 of LA FOIP does not apply, unless there is a compelling reason not to, local authorities should always notify affected individuals of a privacy breach. Affected individuals are in the best position to determine how a privacy breach will affect them.

[40] Page 232 of the *Guide to LA FOIP*, Ch. 6, states that notifications to affected individuals should include the following information:

- A description of the breach (a general description of what happened).
- A detailed description of the personal information involved (e.g., name, credit card numbers, medical records, financial information, etc.).
- A description of possible types of harm that may come to them as a result of the privacy breach.
- Steps taken and planned to mitigate the harm and to prevent future breaches.
- If necessary, advice on actions the individual can take to further mitigate the risk of harm and protect themselves (e.g., how to contact credit reporting agencies).
- Contact information of an individual within your organization who can answer questions and provide further information.
- A notice that individuals have a right to complain to the IPC (provide contact information).
- Recognition of the impacts of the breach on affected individuals and an apology.

[41] Living Sky indicated that it notified students currently attending the Kerrobert Composite High School; however, it did not provide notification to students who graduated in the spring of 2023. Living Sky stated as follows why notification was not provided:

1. The school division does not collect contact information for students once they leave our division.
2. Our PIA investigation indicated that, per the terms of service, six months after a yearbook is locked data for graduated services is deleted, so raw images of these students should not have been involved in the breach, regardless.

[42] Prairie Spirit indicated it posted its notification to its website and to the relevant school community through Edsby, a platform that school divisions use to communicate with students and parents. Horizon advised that it sent an email to the families at both affected schools via School Messenger sharing the notice it received from Edge.

[43] Each of the school divisions provided my office with copies of general notifications. The notifications advised families that their child's photo may have been involved and that the photos had "no other identifying information." However, it is unclear if any of the school divisions identified any specific photos at issue or determined if any metadata was attached to the photos. It does not appear that any school division discussed any potential harm that may result due to the breach, nor advise what actions individuals could take to further mitigate the risk of harm or protect themselves. It also appears that only Prairie Spirit provided contact information for my office.

[44] While the school divisions took steps to notify affected individuals, I find they should have included more information in their notifications to ensure they included all elements my office recommends. This includes the right to make a complaint to my office if not satisfied with the school division's response to the privacy breach.

[45] I recommend that, in the future, the school divisions ensure their privacy breach notifications contains all the recommended elements outlined in my office's [*Privacy Breach Guidelines*](#), when issuing them to affected individuals.

Investigated the breach

[46] Investigating the privacy breach to identify the root cause is key to understanding what happened. Identifying the root cause will help prevent similar breaches in the future. Page 240 of the *Guide to LA FOIP*, Ch. 6, provides that a root cause analysis is a useful process for understanding and solving a problem. It seeks to identify the origin of a problem by using a specific set of steps and tools to:

- Determine what happened.
- Determine why it happened.
- Figure out what to do to reduce the likelihood that it will happen again.

[47] Edge provided my office with a copy of an initial report from Entourage that outlined the following details of the ransomware attack that resulted in the privacy breach:

- As noted earlier in this report, Entourage indicated that on February 5, 2024, its development team recognized an attack its Canadian Amazon Web Services (AWS) cloud server. The result was a ransomware attack where the attackers deleted the contents of a number of its storage buckets that were in use. One of these buckets was the photo storage bucket used by the CreatorStudio Pro application dedicated to Edge. The threat actors then left a message in the emptied storage buckets with instructions that the content of the buckets were downloaded and deleted and they had left emails to contact with instructions on how to pay a ransom for the return of the data.
- Entourage identified the compromised username and password that was used to access the cloud server storage buckets. Entourage identified that the storage buckets containing photos from 400 Edge accounts had been uploaded by the threat actor and deleted from Entourage's cloud server.

[48] Further, Living Sky's Questionnaire provided a copy of a letter dated March 22, 2024, for CreatorStudio Pro, owned by Entourage, that includes highlights from the forensic report following a full forensic review of the yearbook software application in Canada and an extensive forensic audit of all applications, network and processes. The letter indicates that it identified the exact method of the attack and noted it identified how the attackers were able to gain access to the access keys to download and delete the photos in the storage

buckets on Entourage's cloud server. As a result of this, Entourage indicated that its third-party cyber security firms collaborated with its team to prevent further attacks.

[49] Based on the above, I find that Entourage's investigation identified the root cause of the cyberattack and identified steps that could be taken to prevent future incidents.

Taken steps to prevent future breaches

[50] As stated in the *Guide to LA FOIP*, Ch. 6 at page 243, the most important part of responding to a privacy breach is to implement measures to prevent future breaches from occurring. This involves identifying the steps that can be taken to prevent a similar privacy breach. For instance:

- Can your organization create or make changes to policies and procedures relevant to this privacy breach?
- Are additional safeguards needed.
- Is additional training needed.
- Should a practice be stopped.

[51] The information submitted to my office indicated that Entourage had taken steps to prevent future privacy breaches including the following:

- Entourage has engaged with industry leading security professionals to forensically review all servers and network configurations related to the breach and provide findings to Edge.
- Entourage has engaged a security strategy company to review and assist in improving security procedures.
- Updating intrusion detection, monitoring and remediation to prevent future attacks.
- Entourage indicated it would continue to monitor its database and system for evidence of any further breaches or attack.
- Building secure offsite backups of photos stored in the cloud server photo storage buckets.

[52] Based on the details provided, I find that the IMSP, Entourage, has taken appropriate technical steps to prevent future cyberattacks.

[53] However, as noted earlier in this report, it is the responsibility of the school divisions to make certain that its IMSPs are meeting the duty to protect personal information under LA FOIP, as the school divisions retain control of the information. The school divisions' Questionnaires outlined some of the steps that would be taken to prevent future breaches.

[54] Horizon indicated the following changes to its policies and procedures and additional safeguards as follows:

- We are reviewing controls related to engagement of contracts with [sic] on behalf of our principals.
- Training will be update [sic] in the fall to include a debrief of the incident, and to reinforce the requirements for use to be able to conduct a privacy impact assessment when onboarding new IT systems.
- We will be working with schools to identify additional areas where they may be seeking common solutions through a third party service provider. We attempt to manage these agreements centrally, and for all schools typically, which did not occur in this case.
- We provide annual training, and we will be updating the format based on the lessons gained from this process.
- The practice of engaging in these agreements by schools is not authorized, and was never authorized. Contracted will be reviewed centrally in order to provide an appropriate review of their data storage and retention commitments in the agreed terms of the contract.

[55] Living Sky indicated that it would implement the following changes:

- Work with Administrators Council to tighten accountability for schools to follow our existing procedures regarding privacy and use of online software.
- Take an inventory of other third party platforms used in our schools.
- Revise current protocols for Media Release and use of software to ensure that additional permissions are secured when indicated by June 30, 2024.

- Develop a protocol for Yearbook advisors regarding data storage, privacy and permissions by June 30, 2024.

[56] Prairie Sprit indicated that it has since terminated its services with Edge and Entourage. Prairie Spirit also referenced changes made by Entourage but did not outline any changes that the school division has made to prevent future privacy breaches or what additional safeguards may be needed.

[57] As noted earlier in this Investigation Report, Edge reported that Entourage had secured the return of the photos removed by the threat actors during the ransomware attack. However, while Prairie Spirit has indicated it has terminated services with the IMSPs, its investigation report did not indicate if it ensured that the copy of the data was deleted from Entourage's server, or if their data was returned to them.

[58] Entourage's Privacy Policy provides the following regarding the retention of data:

DATA DELETION POLICY

Six months after a yearbook project is locked, we delete all photos (and associated data) uploaded to the project that are not used in the locked project. Thereafter, we only retain the data necessary to allow the adviser to edit the ordered project and/or reorder copies of that project.

When a user deletes a project we retain the data associated with that project for six months to allow for recovery of accidental deletions. Data in a deleted project that is also included in another project will not be deleted.

Furthermore, we adhere to the principles of data avoidance and data economy. Therefore, we only store the personally identifiable data that is necessary to achieve the purposes for which it is provided or as provided for by law. After the expiration of these deadlines, the corresponding data will be blocked or deleted.

With respect to deleting a project or content in a project, 30 days after a written request to delete a project or delete all or a portion of the photos from the project received from an authorized individual at a school or client, Entourage will delete such project, content and associated data.

With respect to deleting a user's account, 30 days after a written request to delete an account from an authorized individual at a school or client, Entourage will delete all personal data including shipping, email and credit card information from the system.

[59] As Prairie Spirit has terminated services with Entourage, it should take steps to ensure its data has been deleted from the IMSPs server, if it has not already done so.

[60] It appears that the school divisions are taking some positive steps towards prevention, such as reviewing its contracts or exploring options with other platforms. When undertaking such steps, I note that section 23.2 of LA FOIP and section 8.2 of *The Local Authority Freedom of Information and Protection of Privacy Regulations* (LA FOIP Regulations) provides as follows regarding a local authority's use of an IMSP:

Section 23.2 of LA FOIP

23.2(1) A local authority may provide personal information to an information management service provider for the purpose of:

- (a) having the information management service provider process, store, archive or destroy the personal information for the local authority;
- (b) enabling the information management service provider to provide the local authority with information management or information technology services;
- (c) having the information management service provider take possession or control of the personal information;
- (d) combining records containing personal information; or
- (e) providing consulting services.

(2) Before disclosing personal information to an information management service provider, the local authority shall enter into a written agreement with the information management service provider that:

- (a) governs the access to and use, disclosure, storage, archiving, modification and destruction of the personal information;
- (b) provides for the protection of the personal information; and
- (c) meets the requirements of this Act and the regulations.

Section 8.2 of the LA FOIP Regulations

8.2(1) For the purposes of clause 23.2(2)(c) of the Act, a written agreement that is entered into between a local authority and an information management service provider must include:

(a) a description of the specific service the information management service provider will deliver;

(b) provisions setting out the obligations of the information management service provider respecting the security and safeguarding of personal information; and

(c) provisions for the destruction of the personal information, if applicable.

[61] Going forward, the school divisions, whether continuing with Edge/Entourage or not, should ensure they have stronger written agreements in place that align with the requirements set out in section 23.2(2) of LA FOIP and section 8.2 of LA FOIP Regulations to protect the personal information involved and ensure compliance. Page 129 of the *Guide to LA FOIP*, Ch. 6, provides that in addition to what LA FOIP and the LA FOIP Regulations require in an information management sharing agreement, there are also some best practices to keep in mind. A well written agreement should also include:

- Identities, roles, and responsibilities of the parties.
- What information is being disclosed and collected and the purpose(s) of each.
- The frequency and duration of information exchanged.
- The legal authority to disclose and collect information.
- The methods and security measures for transferring and storing the information.
- Procedures in the event there is a privacy or security breach.
- Limitations for collection, use, disclosure, and retention.
- Provisions for accuracy of the information.
- Indemnification.
- Compliance monitoring.

[62] I recommend that, going forward, the school divisions ensure they have written agreements with IMSPs in place that address the specific requirements outlined at subsection 23.2(2) of LA FOIP, section 8.2 of the LA FOIP Regulations and the key component for a well written agreement listed at paragraph [61] of this Investigation Report.

[63] As referenced earlier in this report, section 23.1 of LA FOIP provides the local authority's establish policies and procedures to maintain administrative technical and physical safeguards to ensure compliance with its duty to protect personal information. To assist in its duty to protect personal information, I recommend that the school divisions ensure that its policies and procedures clearly sets out the specific requirements in LA FOIP and the LA FOIP Regulations that must be included in a written agreement with an IMSP.

III FINDINGS

[64] I find that I have jurisdiction to conduct this investigation.

[65] I find that there is personal information involved, and that the school divisions have control over the personal information.

[66] I find that a privacy breach occurred.

[67] I find that there was no containment.

[68] I find that the notification to affected individuals was not sufficient as they did not contain all the necessary elements including the right to make a complaint to my office.

[69] I find that Entourage's investigation identified the root cause of the cyberattack and identified steps that could be taken to prevent future incidents.

[70] I find that the IMSP, Entourage, has taken appropriate technical steps to prevent future cyberattacks.

IV RECOMMENDATIONS

- [71] I recommend that, in the future, the school divisions ensure their notification contains all the necessary elements when issuing notification to affected individuals as outlined in my office's, [*Privacy Breach Guidelines*](#).
- [72] I recommend that, going forward, the school divisions ensure they have written agreements with IMSPs in place that address the specific requirements outlined at section 23.2(2) of LA FOIP, section 8.2 of the LA FOIP Regulations and the key component for a well written agreement listed at paragraph [61] of this Investigation Report.
- [73] I recommend that the school divisions ensure that its policies and procedures clearly sets out the specific requirements in LA FOIP and the LA FOIP Regulations that must be included in a written agreement with an IMSP.

Dated at Regina, in the Province of Saskatchewan, this 18th day of September, 2024.

Ronald J. Kruzeniski, K.C.
A/Saskatchewan Information and Privacy
Commissioner