Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 253-2024, 033-2025

Saskatchewan Legal Aid Commission

June 11, 2025

Summary: The Saskatchewan Legal Aid Commission (SLAC) proactively reported a privacy breach to the Office of the Saskatchewan Information and Privacy Commissioner (OIPC). A SLAC employee posted a photograph (photo) to their Facebook and Instagram accounts that disclosed the personal information of 13 SLAC clients. The photo displayed a portion of the employee's work desktop computer with their work email account visible in the background. The personal information of the SLAC clients (affected individuals) was visible in the open work email account. One of the affected individuals (Complainant) made a formal complaint to OIPC. OIPC investigated under *The Freedom of Information and Protection of Privacy Act* (FOIP) and found that a privacy breach occurred for the unauthorized disclosure of the 13 SLAC clients' personal information. The Commissioner made several findings, including: 1) SLAC's response in containing the breach was insufficient; 2) The notice sent to the affected individuals was sufficient because even though there was no mention of the risk of harm caused, in this case the reputational harm was obvious; 3) SLAC adequately addressed the key questions associated with this investigation; and 4) SLAC failed in its objective of future prevention of similar breaches. The Commissioner made several recommendations, all arising from the above findings and she specifically addressed the serious issue of social media and personal employee devices in the workplace.

I BACKGROUND

[1] On October 30, 2024, the Saskatchewan Legal Aid Commission (SLAC) emailed the Office of the Saskatchewan Information and Privacy Commissioner (OIPC) and proactively reported a privacy breach:

> …A [employee][1] at the Saskatoon City Area Office had posted work related photos to [their] social media. One of the photos showed a portion of [their] computer screen which included client names and information about clients.
>
> The employee was instructed to remove the photos and they have been removed from [their] social media.

[2] On October 13, 2024, OIPC requested additional details from SLAC, and SLAC responded on November 18, 2024.

[3] On November 21, 2024, OIPC notified SLAC that it would undertake an investigation. OIPC opened File 253-2024 in relation to SLAC's proactively reported privacy breach.

[4] On December 6, 2024, SLAC provided notice of the privacy breach to the affected individuals.

[5] On December 23, 2024, SLAC provided OIPC with its completed *Privacy Breach Investigation Questionnaire* (Questionnaire)[2], and other relevant documentation.

[6] On January 5, 2025, one of the affected individuals (Complainant) advised OIPC that they were not satisfied with SLAC's response to the privacy breach. On February 10, 2025, the Complainant indicated that they would like OIPC to proceed with an investigation of their complaint. OIPC opened File 033-2025 in relation to the complaint.

[7] On February 20, 2025, OIPC notified SLAC and the Complainant that a complaint file had been opened and that OIPC would likely issue an Investigation Report.

---

[1] The words in square brackets are OIPC's amendments of SLAC's response only to preserve the identity of the employee.

[2] OIPC *Privacy Breach Investigation Questionnaire*: https://oipc.sk.ca/resources/resource-directory/privacy-breach-investigation-questionnaire/.

[8] On May 29, 2025, OIPC informed SLAC that an Investigation Report would be issued for this matter.

II DISCUSSION OF THE ISSUES

1. Does OIPC have jurisdiction?

[9] SLAC qualifies as a "government institution" pursuant to section 2(1)(d)(ii) of *The Freedom of Information and Protection of Privacy Act* (FOIP) and section 3 and PART I of the Appendix of *The Freedom of Information and Protection of Privacy Regulations*.

[10] Therefore, OIPC has jurisdiction to undertake this investigation.

2. Is personal information involved and did a privacy breach occur?

[11] On October 24, 2024, SLAC discovered that one of its employees posted a photo containing the personal information of 13 SLAC clients to their Facebook and Instagram accounts. The posting occurred on September 18, 2024. The photo displayed a portion of the employee's work email that revealed personal information with respect to all 13 SLAC clients. This included the client names and in some instances the following types of information were referenced in the subject line of the email list: the legal services number (LSN) assigned by SLAC, judicial interim release status, date of birth, conditional sentence breach status, pre-sentence report status and future court appearance dates.

[12] A privacy breach occurs when personal information is collected, used and/or disclosed without authority or proper consent under FOIP. Privacy breaches can also occur when personal information is not appropriately safeguarded pursuant to section 24.1 of FOIP or

collected or used in a way that is not accurate nor complete as required by section 27 of FOIP.[3]

[13] The privacy rules in FOIP only apply to personal information.[4] To determine if a privacy breach has occurred, OIPC must first determine if personal information is involved in this matter. If that is the case, then it must be determined if the personal information was collected, used and/or disclosed without the proper authority as granted pursuant to FOIP.

[14] Personal information is defined in section 24(1) of FOIP, though the list is not exhaustive. Personal information is information that is about an identifiable individual, and that is personal in nature. Information is *about* an identifiable individual if the individual can be identified from the information, a common example is if the information includes the name of the individual. Further, and in keeping with basic logic, information is personal in nature if it provides something identifiable about the individual.[5]

[15] SLAC acknowledged that the 13 affected individuals were SLAC clients. SLAC provided OIPC with a copy of the photo the employee posted on their personal Facebook and Instagram accounts. From a review of the photo, two columns of information are visible in the photo. One column contains the names of the sender of the email, the second column contains email subject lines which revealed the topics as listed above in paragraph [11] as it pertained to each individual client.

[16] SLAC provides "legal advice and representation in court to people who cannot afford to pay for services."[6] The disclosure of the names alone would reveal that these individuals were in the course of receiving legal assistance from SLAC. Once again, the subject lines

---

[3] See OIPC Investigation Report 103-2018, 105-2019, 106-2019 at paragraph [25].

[4] see OIPC Investigation Report 129-2024 at paragraph [7].

[5] See OIPC Review Report 005-2025 at paragraph [33].

[6] SLAC website.

reveal information that is personal in nature including client names, date of birth, criminal history, the SLAC LSN assigned to an individual[7] and/or correspondence that may be subject to solicitor/client confidence.[8] These data elements can be defined as personal information by subsections 24(1)(a), (b), (d), (g), (k)(i) and (ii) of FOIP as follows:

> **24**(1) Subject to sections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form, an includes:
>
> (a) information that relates to the race, creed, religion, colour, sex, sexual orientation, family status or marital status, disability, age, nationality, ancestry or place of origin of the individual;
>
> (b) information that relates to the education or the criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
>
> …
> (d) any identifying number, symbol or other particular assigned to the individual, other than the individual's health services number as defined in *The Health Information Protection Act*;
>
> …
> (g) correspondence sent to a government institution by an individual that is implicitly or explicitly of a private or confidential nature, and replies to the correspondence would reveal the content of the original correspondence, except where the correspondence contains the view or opinions of the individual with respect to another individual;
>
> …
> (k) the name of the individual where:
>
> (i) it appears with other personal information that relates to the individual; or
>
> (ii) the disclosure of the name itself would reveal personal information about the individual.

[7] Paragraph [21] of OIPC Review Report 201-2022 found that the LSN SLAC assigns to its clients is personal information pursuant to section 24(1)(d) of FOIP.

[8] Paragraph [17] of OIPC Review Report 201-2022 found that emails sent by an individual to SLAC that is of a private or confidential nature and replies to a request qualified as personal information pursuant to section 24(1)(g) of FOIP.

[17] Therefore, it is clear this matter involved "personal information" as defined by subsections 24(1)(a), (b), (d), (g), (k)(i) and (ii) of FOIP.

[18] Section 29(1) of FOIP states as follows:

> **29**(1) No government institution shall disclose personal information in its possession or under its control without the consent, given in the prescribed manner, of the individual to whom the information relates, except in accordance with this section or section 30.

[19] Section 29(1) of FOIP prohibits disclosure of personal information unless proper consent is obtained prior to disclosure. Section 29(2) and section 30 of FOIP authorize disclosure absent consent in instances where the individual is deceased or in certain legal or investigative situations where the state is involved, none of which apply here. FOIP does not define the term "disclosure". OIPC has defined "disclosure" as the sharing of personal information with a separate entity, not a division or branch of the public body in possession or control of that record/information.[9]

[20] In this case, posting this photo to the employee's Facebook and Instagram accounts is a "disclosure" of the SLAC clients' personal information. There will be a finding that a privacy breach occurred for the unauthorized disclosure of the personal information of the 13 SLAC clients. This disclosure was without consent and outside the parameters of section 29(1) of FOIP.

3. Did SLAC respond to the privacy breaches appropriately?

[21] The determination of the appropriateness of a government institution's response to a privacy breach involves several considerations. Whether the government institution appropriately responds to a privacy breach and takes proper corrective measures is

[9] See OIPC Investigation Report 083-2023 at paragraphs [13] and [14]; see also *Saskatchewan Information and Privacy Commissioner 2007-2008 Annual Report* at page 71.

informed by sections 6-7 and 7-7 of OIPC's *Rules of Procedure*. The following considerations include:

i. Was the breach contained;

ii. Were the affected individuals notified;

iii. Was the breach investigated; and

iv. Were appropriate steps taken to prevent future breaches.

i. Containment of the Breach

[22] Upon learning that a privacy breach has occurred, government institutions should take *immediate* steps to contain the breach. These steps will depend entirely upon the nature of the breach, but they may include: [10]

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

[23] OIPC applies a standard of reasonableness to assess the containment of a breach. The institution must demonstrate that it has reduced the magnitude of the breach and the resulting risk to affected individuals. This measure serves as a reassurance to the public and, most of all, the clients they serve.[11] A privacy breach is a very serious matter. A privacy breach always results in a loss of faith and trust on the part of the public in the

[10] See OIPC Investigation Report 083-2023 at paragraph [22]; see also OIPC's resource, *Privacy Breach Guidelines for Government Institutions and Local Authorities*.

[11] See OIPC Investigation Report 197-2022, 215-2022 at paragraph [19].

institution, and a loss of faith and trust on the part of the clients the institution serves. In the case of SLAC this is very serious because of the services SLAC provides the public.

[24] In its completed Questionnaire, SLAC provided the following regarding the timeline of events and the steps it took to contain the breach:

> A [employee] at the Saskatoon City Area Office had posted work related photos on [their] social media. One of the photos showed a portion of [their] computer screen which showed [their] email account that showed client names and information about clients.
>
> An LAS employee noticed the posts on the evening of October 23, 2024 and notified LAS People and Culture on October 24, 2024. The employee who posted the photo confirmed the photo was posted on their Facebook and Instagram accounts on September 18, 2024. The accounts were public at that time.
>
> The employee was instructed to remove the photos. The employee confirmed to the Administrative Staff Manager that the photos were removed as of October 28, 2024. The accounts, that were public at the time of the posting, are now private.
>
> The employee also confirmed to the Administrative Staff Manager that the photos were deleted from [their] devices.
>
> There is no indication the photos were downloaded or shared.

[25] SLAC posed questions to the employee in an effort to assess the exact nature of the breach and how to contain it. SLAC's questions and the employee's responses are provided below:

1. **Were the screenshots on both Facebook & Instagram or just one?**

   Screenshots were from both Facebook and Instagram

2. **When did you remove them?**

   I removed them on Monday October 28th

3. **Screenshots were posted on the days you noted in your email. Were they available to the public until the day they were removed or just a 24-hour period?**

> They were available to the public until the day they were removed. I had them on my Instagram highlight, so anyone had access even though some of them were from months ago.
>
> **4. To confirm; you had no other LAS related posted on your social media?**
>
> Correct, no other LAS related posts posted to my social media
>
> **5. On average how many people view your reels?**
>
> On average, I get 60-100 views on my Instagram stories (in the 24 hour period). I did not post any Reels related to LAS, the Reels I have posted in the past got anywhere from 100-950 views but again wasn't in respect to LAS only personal life stuff...

[26] Several factors would have limited SLAC's ability to contain the breach, which are explained in the paragraphs that follow. The overall goal must be to contain the breach as much as possible and as soon as possible, so as to lessen its negative impact. This is the "reasonable response" analysis

[27] The photo was displayed on the employee's Facebook and Instagram accounts for over a month, since the investigation revealed that the employee first posted the photographs on September 18, 2024. The breach came to the attention of SLAC by means of a report on the part of another employee who recognized the information displayed and the serious nature of the unauthorized disclosure (reporting employee). The length of time the photo was available to the public for view is considerable when one thinks of the fact that online postings allow viewers ample time to share, copy, screenshot and retain.[12]

[28] With respect, even though SLAC stated in their response that: "there is no indication the photos were downloaded or shared", there is no way of verifying whether there were downloads or sharing of the impugned photograph. Individuals who viewed the posts could have captured a screenshot of the photo or jotted down information from it and no one would ever know. This is a risk that affects the ability of any organization to absolutely

[12] Paragraphs [32] to [35] of OIPC Investigation Report 154-2022 discuss issues with lapsed time in the containment of a breach.

contain a privacy breach of this nature. Because of the length of time the photo was on public display, the containment of the breach must be considered to have been seriously jeopardized – if not impossible. Further, there is no evidence that SLAC took steps to inquire and ensure that the reporting employee did not make copies of the impugned posting. While the reporting employee is a very responsible and loyal employee, the government institution must take every step to contain the breach, and this includes the making of such an inquiry.

[29] Finally, there is the disturbing issue of online content that can never be permanently deleted. The Northwest Territories Information and Privacy Commissioner (NWT IPC) dealt with a similar privacy breach in Review Report 20-HIA 34. In that report, the NWT IPC considered how Facebook manages information even if an employee deletes the information they have shared on Facebook. It is helpful to review Facebook's policy with respect to deleted content: [13]

> When you choose to delete something you shared on Facebook, we remove it from the site. Some of this information is also permanently deleted from our servers and backup systems so we may not be able to retrieve deleted content in these cases. Some deleted information lives on our backup systems even though it is no longer visible on Facebook and can only be fully removed when you permanently delete your account.
>
> [Emphasis added]

[30] Facebook and Instagram are owned by the same parent company, META. Instagram's policy states the following with respect to deleting Instagram content:[14]

> Content that you choose to delete is removed from your account immediately and moved to Recently Deleted.

[13] Facebook Help Center: What happens to content (posts, pictures) that I delete from Facebook | Facebook Help Center.

[14] Instagram Help Center: What happens to content you've deleted from your Instagram account | Instagram Help Center.

> Content in Recently Deleted will be automatically deleted 30 days later, or up to 24 hours for stories that aren't in your stories archive. During those 30 days, you can access deleted content from your account in Recently Deleted on the Instagram app for Android and iPhone and either restore it or permanently delete it.
>
> During those 30 days the content remains subject to Instagram's Terms of Use and Privacy Policy and is not accessible to other people using Instagram.
>
> It may take up to 90 days to complete the deletion process after it begins. Copies of your content may remain after the 90 days in backup storage that we use to recover in the event of a disaster, software error, or other data loss event. We may also keep your information for things like legal issues, terms violations, or harm prevention efforts.
>
> [Emphasis added]

[31] A review of Facebook and Instagram policies clearly reveal that deleting or de-activating an account does not guarantee the deletion of content posted to these accounts.[15] Quite simply, there is no guarantee that online content is ever truly deleted. The content may linger in some unknown way on META's servers which are located around the world. Personal information that exists on servers outside Canada is subject to the laws of those jurisdictions and beyond the scope and control of our sovereign Canadian laws.[16] Facebook and Instagram have different deletion processes. The nature of how each social media entity manages deleted content is a serious concern that negatively impacts the ability of a government institution to contain a privacy breach such as this.

[32] SLAC's Privacy Officer explained that on Friday, October 25, 2024, an email was received from a Director at SLAC advising of the posting and the fact that the employee had been instructed to remove the posts immediately. Upon the employee's return to work on Monday October 28, 2024, SLAC took steps to have the employee remove the photo from their social media accounts and their personal devices. These were important measures on

---

[15] Facebook Help Center: Permanently delete your Facebook account | Facebook Help Center; Instagram Help Center: Permanently delete or deactivate your Instagram account | Instagram Help Center.

[16] See OIPC Investigation Report 101-2017 at paragraph [27].

the part of SLAC. Still, SLAC should also have ensured that the reporting employee did not possess any copies or screenshots.

[33] The goal of containment is to stop the spread of the breach and if that is not possible, to minimize the spread of the breach to the extent possible. There will be a finding that SLAC's response in containing the breach was insufficient in that the reporting employee was never asked if copies were made. There will be a recommendation that, within 30 days of the issuance of this Investigation Report, SLAC verify that the reporting employee is not in possession of any screenshots or reproductions of the impugned posting.

ii. Notification of Affected Individuals

[34] It is best practice for government institutions to inform affected individuals as soon as possible when their personal information and/or personal health information has been breached. This is an obvious and crucial step that invokes the principles of fairness. Affected individuals must be informed of the possible risks so they can take any remedial steps they deem necessary to protect themselves.[17]

[35] Section 29.1 of FOIP requires government institutions to notify individuals when their personal information has been breached and a real risk of significant harm exists for the affected individual.[18] Section 29.1 of FOIP states:

> **29.1** A government institution shall take all reasonable steps to notify an individual of an unauthorized use or disclosure of that individual's personal information by the government institution if it is reasonable in the circumstances to believe that the incident creates a real risk of significant harm to the individual.

[17] See OIPC Investigation Report 290-2024, 007-2025 at paragraph [24]; see also OIPC's resource *Privacy Breach Guidelines for Government Institutions and Local Authorities*.

[18] See OIPC Review Report 129-2024 at paragraph [28].

[36] The information that a government institution should include in a notice to an affected individual(s) may include:[19]

- 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 OIPC (provide contact information).
- Recognition of the impacts of the breach on affected individuals and an apology.

[37] On December 6, 2024, SLAC sent letters to the affected individuals to notify them of the privacy breach. The letters included:

- A description of how the breach occurred;
- The personal information disclosed for each SLAC client;
- The steps taken to contain the breach;
- The contact information for SLAC's Privacy Officer;
- The fact that the breach had been reported to OIPC;
- That affected individuals had the right to make a complaint to OIPC;
- OIPC's contact information; and

[19] See OIPC Investigation Report 129-2024 at paragraph [32].

- An apology.

[38] SLAC's notices to the affected individuals covered many of the recommended elements in paragraph [36] above, and we commend SLAC on this. When a privacy breach occurs, a government institution should also advise individuals of the possible types of harm that may result, which is typically linked to the nature of the personal information breached. In its submission, SLAC identified this was a breach that could lead to "reputational" harm. Since this harm is obvious from the nature of the breach and the items that were disclosed in paragraph [11] of this report, OIPC will not recommend that SLAC notify the affected clients of potential reputational harm.

[39] However, and in going forward, when a privacy breach occurs, it is good policy to inform the victim of the breach of the type of harm that can occur unless it is patently obvious as in this case. There will be a recommendation that within 30 days of the issuance of this Investigation Report, SLAC develop a policy or procedure for assessing the risk of harm when a privacy breach occurs and actions to take to mitigate those risks. In so doing, SLAC may refer to risk assessment tools that assist organizations in assessing risks to individuals and the likelihood of harm resulting from the breach.[20]

iii. Investigation of the Privacy Breach

[40] Once a privacy breach has been contained and appropriate notification has been given, the government institution should conduct an investigation. The investigation must address the incident on a systemic basis and include a root cause analysis. The institution must consider its duty to protect personal information as set out at section 24.1 of FOIP. Specifically, section 24.1 of FOIP requires that government institutions establish policies and procedures to maintain administrative, technical and physical safeguards:

[20] See Office of the Privacy Commissioner of Canada's tool for assessing if a privacy breach poses a real risk of significant harm to an individual: https://www.priv.gc.ca/en/privacy-topics/business-privacy/breaches-and-safeguards/privacy-breaches-at-your-business/rrosh-tool/.

> **24.1** Subject to the regulations, a government institution 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.

[41] In assessing the root cause of a privacy breach, the government institution must formulate safeguards that would have prevented the privacy breach from occurring in the first place.[21] Safeguards can be administrative (e.g., policies, procedures, confidentiality statements on contracts), technical (e.g., access controls on electronic storage) or physical safeguards (e.g., locked cabinets or bins, locked doors, security cameras).

[42] Some key issues to consider in determining the proper safeguards include: [22]

- When and how did your organization learn of the privacy breach?
  - Has the privacy breach been contained?
  - What efforts has your organization made to contain the breach?

[21] See OIPC Investigation Report 290-2024, 007-2025 at paragraph [33]; see also OIPC's resource *Privacy Breach Guidelines for Government Institutions and Local Authorities*.

[22] See OIPC Investigation Report 266-2024, 031-2025 at paragraph [66]; see also OIPC's resource *Privacy Breach Guidelines for Government Institutions and Local Authorities*.

- What occurred?

  - What type of breach occurred (e.g., collection, use, disclosure, accuracy, etc.)?
  - What personal information was involved in the privacy breach?
  - When did the privacy breach occur? What are the timelines?
  - Where did the privacy breach occur?

- How did the privacy breach occur?

  - Who was involved?
  - What employees, if any, were involved with the privacy breach?
  - What privacy training have they received?
  - Who witnessed the privacy breach?
  - What factors or circumstances contributed to the privacy breach?
  - What is the root cause of the breach?

- What is the applicable legislation and what specific sections are engaged?

- What safeguards, policies, and procedures were in place at the time of the privacy breach?

- Was the duty to protect met?

  - Were the safeguards, policies, and procedures followed?
  - If no safeguards, policies, or procedures were in place, why not?
  - Were the individuals involved aware of the safeguards, policies, and procedures?

- Who are the affected individuals?

  - How many are there?
  - What are the risks associated to a privacy breach involving this information (e.g., is the affected individual at risk for identity theft, credit card fraud, etc.)?
  - Have affected individuals been notified of the privacy breach?

[43] SLAC provided details of its interview with the employee who committed the privacy breach. The details are provided in paragraph [25] above. In its interview notes, SLAC noted that the employee acknowledged that this was a "breach of confidentiality," had expressed remorse and took responsibility for their actions. For its part, SLAC stated that it did not believe the employee's act was malicious or intended to be harmful to the organization. SLAC relayed that it reminded the employee that they had signed a

confidentiality policy on February 1, 2024 and their action in posting the photo was a clear violation of that policy. SLAC also informed the employee that the privacy breach did not align with SLAC's values, which include ethical practice and integrity.

[44] SLAC reported the employee completed privacy training on July 12, 2024 – just two months before the posting that led to this breach. SLAC added that when the privacy breach occurred, it had several relevant policies and procedures in place, which it provided to this office for review:

> *Client Information Management Policy* (revised January 2019);
>
> *Legal Aid Saskatchewan IT Security Policy* (effective June 18, 2024);
>
> *Legal Aid Saskatchewan IT Usage Policy* (effective June 18, 2024);
>
> *Saskatchewan Legal Aid Commission Code of Employee Conduct* (amended June 21, 2022), which outlines the correct use of social media; and
>
> *Legal Aid Saskatchewan Confidentiality Policy*, which the employee had signed February 1, 2024.

[45] SLAC's *IT Usage Policy* provides the following:

> **Acceptable Use of User Accounts**
>
> …
> To ensure the security and privacy of user accounts, this policy outlines the measures and protocols in place to protect users' information from unauthorized access, breaches and misuse.
>
> This policy provides an assured framework within which the security, confidentiality, integrity and safe use of data and information is maintained:
>
> …
> - data and information are not disclosed to those without the authority to use it;
>
> …
> **Acceptable Use of LAS Email**
>
> …This policy also provides an assured framework within which security, confidentiality, integrity and safe use of data and information is maintained:

- data and information are available only to those authorized to view it;
- data and information are not disclosed to those without the authority to use it;

[Emphasis added]

[46] SLAC's *Code of Employee Conduct* also provides some guidance on the use of social media and protection of personal information:

> **5. Social media**
>
> …
> While social media can be a valuable tool of information in our everyday lives, social media usage may have damaging (actual or potential) effects on our employees, clients and LAS's reputation.
>
> LAS prohibits the use of unauthorized social media during work hours, on an approved LAS work location or property, or on organizational equipment. Employees should consult their Director or the Director of Finance & IT with their questions about acceptable use.
>
> …
> If the employee publishes comments that are harassing to coworkers or reflect badly on LAS, even if it is on their personal social media, on their personal time, disciplinary action may be warranted**.**
>
> …
> LAS provides some flexibility for allowing employees to access social media sites such as Facebook on an LAS device, but this should be limited to unpaid breaks.
>
> …
> **6. Information Technology**
>
> All employees must be aware of their obligations and responsibilities regarding the security of data…
>
> Policies are in place to protect the personal and privileged information of our clients and employees…
>
> …

> **7. Confidentiality and records management**
>
> Legal Aid Saskatchewan is subject to the *Freedom of Information and Privacy Act*…
>
> Employees shall not disclose to any member of the public, either orally or in writing, any confidential information acquired by virtue of their official position, except when reasonably required by law.
>
> [Emphasis added]

[47] SLAC's *Code of Employee Conduct* provides valuable guidance to employees regarding the use of social media; however, it could be clearer on what is and is not acceptable use of social media by employees. There should be a clear statement that the use of social media and personal devices by employees are both strictly forbidden during work hours and when using SLAC technology.

[48] SLAC conceded the employee did not follow policy with respect to confidentiality and information security and that the employee demonstrated a lack of judgement in posting work photos and specifically this particular photo. A negligent employee was the root cause of the privacy breach. This employee failed to follow privacy training and failed to adhere to SLAC's policies for protecting the personal information of its clients.

[49] In conclusion, there will be a finding that SLAC has adequately addressed the key issues associated with this investigation.

iv. Prevention of Future Breaches

[50] It is crucial to ensure the implementation of vital measures so as to prevent similar breaches from occurring in the future. Possible prevention measures may include adding/enhancing safeguards already in place, providing additional training, and the regular

monitoring/auditing of systems and system users.[23] The following considerations are relevant: [24]

- 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] In spite of the fact the employee acknowledged their actions caused the privacy breach, SLAC required the employee to take remedial privacy training which was completed on December 23, 2024, two months after the discovery of the privacy breach.

[52] This office reviewed the remedial privacy training program and noted a glaring omission. The SLAC remedial training program fails to address the dangers of social media in the workplace. There will be a recommendation that remedial training occur as soon as possible after a breach if the root cause is an employee. There will also be a recommendation that remedial privacy training cover the dangers of social media in the workplace.

[53] The only consequence for the employee at the root cause of this privacy breach was remedial training. This privacy breach was especially serious in terms of the vast reputational harm to which the victims were subject. Disciplinary action is not to be considered as a punitive measure, but it should be considered as a reprimand and a message that unauthorized disclosure of personal information has to be accompanied by consequences. It is important that institutions consider disciplinary action in instances

[23] See OIPC Investigation Report 290-2024, 007-2025 at paragraph [35]; see also OIPC's resource *Privacy Breach Guidelines for Government Institutions and Local Authorities*.

[24] See OIPC Investigation Report 266-2024, 031-2025 at paragraph [72]; see also OIPC's resource *Privacy Breach Guidelines for Government Institutions and Local Authorities*.

where policies and procedures are not followed.[25] This office discussed the topic of disciplinary action in response to a privacy breach that is the sole result of employee negligence:[26]

> [34] In Investigation Reports 088-2013 and 100-2015, I stated that disciplinary actions should be strong enough that it deters individuals from intentionally breaching personal data. Those reports involved personal health information, but in my view, the type of data in the possession of political parties may be as sensitive as personal health information and therefore warrants strong disciplinary actions as well.

[54] SLAC's *Code of Employee Conduct* states that an employee may be subject to discipline if they publish comments, including to social media, that are "harassing of coworkers or reflect badly on LAS". In connection with this code of conduct and in order to support effective, consistent discipline when an employee breaches privacy, a model for discipline review should be considered to determine levels of a breach (e.g., unintentional, malicious), and actions to be taken by the employer depending on the level of breach. An excellent example is the matrix developed by the Saskatchewan Health Authority (SHA) entitled: "Privacy Incident Management Procedure."[27] There will be a recommendation that within 30 days of the issuance of this Investigation Report, SLAC develop a model for discipline review similar to the matrix provided by SHA and consider whether further disciplinary action is warranted in the present situation.

[55] In its discussions with this office, SLAC indicated that it intended to provide privacy training for all staff and that it would focus on the prevention of privacy breaches in the future. The policies related to this situation and privacy issues in general are under review and will be completed by the end of the summer. The use of employee personal devices and social media in the workplace is a very important topic as the internet has subsumed most office practices. It is crucial that all stakeholders take sufficient steps to safeguard the

---

[25] See OIPC Investigation Report 126-2019, 137-2019, 182-2019, 191-2019 at paragraph [19].

[26] See OIPC Investigation Report 093-2018 at paragraph [34].

[27] Appendix B of the Saskatchewan Health Authority's *Privacy Incident Management Procedure*.

personal information of the people they serve. In this case the individuals who come to SLAC for legal assistance rely on absolute confidentiality as they face a very difficult period in their lives. Employees of SLAC should fully understand that they are not to use their personal devices or access social media in the workplace during work hours.[28] As noted earlier in this Investigation Report, SLAC's *Code of Employee Conduct* provided some guidance on the use of social media, however it does not clearly delineate the issue of social media in the workplace. When a privacy breach occurs, a government institution should immediately take steps to address gaps in its safeguards to prevent future occurrences. I recommend that within 30 days of the issuance of this Investigation Report, SLAC finalize additional guidance for its *Code of Employee Conduct* on acceptable and unauthorized use of social media and require all employees to review and sign.

[56] SLAC may also want to consider guidance from the Office of the Privacy Commissioner of Canada regarding privacy and social media in the workplace when developing this additional guidance for its *Code of Employee Conduct*:

> **Consequences of inappropriate disclosure on social media**
>
> Employers and employees should be aware of the potential damages to individuals and the corporation through inappropriate disclosures of personal or confidential business information on social media. The possible consequences of an improper or unintended disclosure may be:
>
> - a defamation lawsuit;
> - copyright, patent or trademark infringement claims,
> - a privacy or human rights complaint;
> - a workplace grievance under a collective agreement or unfair labour practice complaint;
> - criminal charges with respect to obscene or hate materials;
> - damage to the employer's reputation and business interests.

[28] See OIPC's resource Helpful Tips: Mobile Device Security.

Legal responsibility for damages from an inappropriate disclosure could potentially rest with individual employees, management or the organization as a whole.

Employers: Develop and communicate a clear policy on social media

While many employers have guidelines and codes of conduct for e-mail and Internet use, social media poses different privacy challenges which should be specifically addressed in conjunction with these other workplace rules. Clear rules and policies drafted specifically on the use of social media should be communicated to all employees.

The policy should generally establish best practices and outline expectations for acceptable use of social media in the workplace, set out the consequences of misuse, and address any workplace privacy issues.

Specifically, the policy should address:

- whether the organization permits the use of personal or employer-hosted social media in the workplace;
- if social media accounts are permissible, in what context and for what purposes may they be used?
- whether the employer monitors social media sites;
- what legislation applies to the collection, use or disclosure of personal information in the workplace;
- what other rules may apply to the use of social media in the workplace (collective agreements; other relevant legislation);
- the consequences of non-compliance with the policy and,
- any other existing policies about the proper use of electronic networks with respect to employee privacy and handling confidential information.

Determine what data should not be disclosed

Employers should inform employees in plain language why it's important to keep some personal and corporate information – about themselves, their co-workers, clients and the organization – confidential or undisclosed. Similarly, employers need to exercise judgment and abide by applicable privacy and other legislation if they decide to collect, use or disclose personal information from social media sources. A privacy-friendly workplace calls for fair use of information by all parties.

[57] There will be a finding that SLAC has failed in its objective of future prevention of similar breaches.

III FINDINGS

[58] OIPC has jurisdiction to undertake this investigation.

[59] A privacy breach occurred for the unauthorized disclosure of the 13 SLAC clients' personal information.

[60] SLAC's response in containing the breach was insufficient.

[61] SLAC's notices to the affected individuals was sufficient because even though there was no mention of the risk of harm caused, in this case the reputational harm was obvious.

[62] SLAC adequately addressed the key questions associated with this investigation.

[63] SLAC failed in its objective of future prevention of similar breaches.

IV RECOMMENDATIONS

Re: Containment of the Breach

[64] I recommend that within 30 days of the issuance of this Investigation Report, SLAC verify that the reporting employee did not retain screenshots or reproductions of the impugned photo.

Re: Notification of Affected Individuals

[65] I recommend that within 30 days of the issuance of this Investigation Report, SLAC develop a policy or procedure for assessing the risk of harm when a privacy breach occurs and actions to take to mitigate those risks.

Re: Prevention of Future Similar Breaches

[66] I recommend that remedial training occur as soon as possible after a breach if the root cause is an employee.

[67] I recommend that in the future, and for breaches of this nature, remedial privacy training include the dangers of using personal devices and accessing social media in the workplace and during work hours.

[68] I recommend that within 30 days of the issuance of this Investigation Report, SLAC develop a disciplinary matrix. I further recommend that SLAC consider whether further disciplinary action is warranted in this situation.

[69] I recommend that within 30 days of the issuance of this Investigation Report, SLAC develop additional guidance for its *Code of Employee Conduct* on acceptable and unauthorized use of social media and require all employees to review and sign.

Dated at Regina, in the Province of Saskatchewan, this 11th day of June, 2025.

Grace Hession David
Saskatchewan Information and Privacy Commissioner