Office of the
Saskatchewan Information
and Privacy Commissioner

REVIEW REPORT 007-2019

Ministry of Central Services

March 17, 2020

Summary: The Ministry of Central Services (Central Services) received an access to information request from the Applicant for personal emails sent and received from their Government of Saskatchewan email account. Central Services responded that the emails were not in its possession or control for the purposes of *The Freedom of Information and Protection of Privacy Act* (FOIP). The Commissioner found that any emails sent or received by the Applicant constituting their personal emails, that are retained on the backup tapes, are not in the possession or control of Central Services for the purposes of FOIP. The Commissioner recommended that Central Services develop and implement a policy to transfer any future requests to the government institution that may have the emails, if they still exist. The Commissioner also recommended that Central Services encourage government institutions to develop and implement a policy or procedure on the management of emails, including regularly saving emails to appropriate locations and deleting personal or transitory emails.

I BACKGROUND

[1] On April 5, 2018, the Ministry of Central Services (Central Services) received an access to information request from an Applicant seeking personal emails that they had sent and received from their Government of Saskatchewan email account from 2004 to the date their employment with the Ministry of Environment (Environment) ceased. The Applicant requested emails from specified senders, emails related to specified topics, and listed a number of personal email folders.

[2] On May 1, 2018, the Central Services responded to the Applicant stating, "we have determined any records related to your request are personal emails that are outside the scope of FOIP and not in our possession or control. Therefore FOIP does not apply."

[3] On January 3, 2019, the Applicant requested a review of Central Services' decision to refuse the Applicant access to the records on the basis that the records were not in its possession or control.

[4] On January 9, 2019, my office notified the Applicant and Central Services of my intention to undertake a review.

II RECORDS AT ISSUE

[5] Central Services has taken the position that it does not have responsive records in its possession and/or control. As such, there are no records at issue in this review. However, it is clear we are discussing the personal emails of the Applicant.

III DISCUSSION OF THE ISSUES

1. Does my office have jurisdiction in this matter?

[6] Central Services qualifies as a government institution pursuant to subsection 2(1)(d)(ii) of *The Freedom of Information and Protection of Privacy Act* (FOIP). Therefore, I have jurisdiction to conduct this review.

2. Are there records responsive to the Applicant's request in the possession and/or control of Central Services?

[7] Section 5 of FOIP provides the right of access as follows:

> **5** Subject to this Act and the regulations, every person has a right to and, on an application made in accordance with this Part, shall be permitted access to records that are in the possession or under the control of a government institution.

[8] As section 5 of FOIP provides that FOIP only applies to those records under the possession or under the control of a government institution, I will need to determine if the records in question would be in the possession or control of Central Services.

[9] The Applicant's submission referred to two factors my office considers for assessing control of records and asserted that Central Services had some measure of control. The two factors that the Applicant relied on to support their position were:

- The public body possesses the record, either because it has been voluntarily provided by the creator or pursuant to a mandatory or statutory or employment requirement; and
- The public body paid for the creation of the records.

[10] The Applicant indicated that Central Services possessed the records as they were the creator of the records, voluntarily provided them and as a former employee of the Government of Saskatchewan, their salary and the resources of the government were "used in the creation and maintenance of the records." Additionally, the Applicant stated that, "the Government of Saskatchewan's Information Technology Acceptable Usage Policy acknowledges that incidental personal use is acceptable, even though the emails themselves are not official records of the government." Finally, the Applicant indicated that personal records that had been saved on a government network drive had been released to them. As the Applicant had gained access to some records, they questioned why the government was acting inconsistently and refusing to provide their personal emails.

[11] Central Services' submission quoted a number of court decisions and referenced my office's Review Report F-2014-007 to support its position that these records were not in the possession or control of Central Services. In that report, my office found that FOIP did not apply as the Ministry "does not have 'control' of the records in question. The emails are the personal records of the government employee and were not created as part of [their] employment duties."

[12] In Review Report 096-2015 and 097-2015, my office found that personal emails of an employee of the Saskatchewan Transportation Company (STC) were not in the possession or control of STC, for the purposes of FOIP, as "the personal records of the STC employee and were not created as part of their employment duties."

[13] In the Provincial Archives of Saskatchewan's resource *Basic Records Management Practices for Saskatchewan Government*, it defines non-public (non-government) records as "records that do not pertain to any aspect of Government business. These include records such as external publications and non work related records (personal e-mails or letters, memberships in associations or groups etc. which do not relate to the employees position within the organization)."

[14] As such, there is no requirement in *The Archives and Public Records Management Act* for a government institution to retain an employee's personal emails, as they are not an official record of the government.

[15] Central Services also noted that the Applicant may have been referred to Central Services to inquire about retrieving the requested emails from the Information Technology Division (ITD) backup tapes. Central Services further clarified that, "email accounts are retained [by Central Services] for system recovery purposes… there is no way for us to distinguish which emails on the backups are personal in nature."

[16] In my office's Investigation Report 072-2018, my office undertook an investigation into Central Services' ITD backup tapes. In that report, I provided the following regarding the purpose of these backup tapes:

> [40] …backup tapes managed by Central Services contain only copies of uncategorized and critical data that already exists elsewhere within one of the twenty-seven clients of Central Services. The original copy of the data should be appropriately stored and retained in accordance with existing legal and policy requirement related to the management of records within the Government of Saskatchewan. If appropriate records management practices exist, then any one of the twenty-seven clients of Central Services who receives an application for access to records under FOIP should be able to conduct a reasonable search for responsive records, regardless of what may or may not exist on backup tapes managed by Central Services.

> [41] The sole purpose of copying digital data that already exists elsewhere onto a backup tape is to allow Central Services to restore the data in case of a major disaster or IT system malfunction…
> …
>
> [45] … in regards to possession or control of records, it is reasonable to accept that Central Services, not its clients, is in possession and control of the data stored on backup tapes. This is because Central Services plays the principal role in:
>
> - Creating the copies of data stored on backup tapes;
> - Establishing when backups are created and how;
> - Using backups in case of a disaster for recovery purposes; and
> - Overseeing the overall management of backup tapes and the data on those tapes.
>
> [46] In light of the above, I find that the data that resides on backup tapes is not the "primary record" that falls within the meaning of subsection 2(1)(i) of FOIP; I find that this data is merely a copy of the data that already exists elsewhere, and it serves a completely different purpose. Accordingly, the data that already exists elsewhere, the original copy of the data, is in fact the "primary record" that would be responsive to an application for access to records under FOIP.
>
> [47] Since data stored on backup tapes is not the "primary record" that falls within the meaning of subsection 2(1)(i) of FOIP, I find that backup tapes do not need to be included in a search for responsive records when processing an application under FOIP. FOIP imposes on government institutions a duty to assist requirement that in part requires institutions to make every reasonable effort to identify and seek out responsive records. However searching within backup tapes exceeds the reasonable efforts required by the duty to assist requirement…

[17] As the Applicant was a former employee of Environment seeking access to their personal emails sent and received during their employment with Environment, my office asked Central Services to clarify if there was any consideration in transferring the request to Environment pursuant to section 11 of FOIP. Section 11 of FOIP provides:

> **11**(1) Where the head of the government institution to which an application is made considers that another government institution has a greater interest in the record, the head:
>
> (a) may, within 15 days after the application is made, transfer the application and, if necessary, the record to the other government institution; and
>
> (b) if a record is transferred pursuant to clause (a), shall give written notice of the transfer and the date of the transfer to the applicant.

> (2) For the purposes of this section, a government institution has a greater interest in a record if:
>
> (a) the record was originally prepared in or for the government institution; or
>
> (b) the government institution was the first government institution to obtain the record or a copy of the record.
>
> (3) For the purposes of section 7, an application that is transferred pursuant to subsection (1) is deemed to have been made to the government institution on the day of the transfer.

[18] Central Services responded stating, "yes, we had considered transferring the request at the time. In speaking with Environment around the possibility of transferring the request, they identified that the former employee's email account was deleted and they did not have access to the personal emails from the former email account."

[19] The purpose of email backups retained by Central Services are for system recovery purposes. I find that any emails sent or received by the Applicant constituting their personal emails, that are retained on the backup tapes, are not in the possession or control of Central Services for the purposes of FOIP.

[20] I recommend that Central Services develop a policy or procedure to ensure access to information requests seeking emails from email backups are transferred to the appropriate government institution that may have the emails, if they still exist.

3. What records management best practices should government institutions have in place for personal emails?

[21] The Government of Saskatchewan *Information Technology Acceptable Usage Policy Email Appendix B*, provides the following guidance:

> Email that is of a personal or transitory nature need not be archived. However, email that is official record of government is to be retained. Remember that email is accessible under the terms of *The Freedom of Information and Protection of Privacy Act*.
> …

> …The email system is the property of the Saskatchewan Government. Employees should have no reasonable expectation of privacy in email transmitted, received and stored on and/or through the governments system. An email is the property of the Government of Saskatchewan and is not a private employee communication (whether created or received).
> …
>
> …Employees are encourage to create separate signature files for personal and official email that is sent from government accounts… Personal signature file text must contain a disclaimer indicating that the email does not represent the views of the Government of Saskatchewan…

[22] While the government's policy is to allow employees use of their government email accounts to send and receive personal emails, government institutions should also be providing guidance on the proper management of emails to ensure emails that are official government records and emails that are transitory or personal emails are managed appropriately.

[23] The Provincial Archives of Saskatchewan resource *Email Management Guidelines*, provides the following guidance on the management of emails:

> Government institutions must ensure that employees understand their records management responsibilities in regard to email and, as part of their records management program, develop the policy and procedures necessary to manage them appropriately.
> …
>
> As is the case for all other government records, email must be classified, retained and disposed of in accordance with an applicable approved retention schedule. Ideally, emails should be classified and retained alongside other records that pertain to the activity or business transaction.
> …
>
> **Email Management Best Practices**
>
> **Regularly Delete Transitory and Non-Work Related Email Messages**
> As previously explained, transitory and non-work related records do not need to be classified and retained. For further information on transitory records, please refer to the Archives' Transitory Records Guidelines.
> …

> **Identify Who is Responsible For a Message**
> Because it is common for multiple copies of an email message to exist, it is helpful to set some guidelines that establish who is responsible for managing messages in different circumstances.
> …
>
> **Roles and Responsibilities**
> Individuals at all levels of the institution have a role to play if email is to be properly managed.
> …
>
> **All Staff**
> - understand and comply with the institution's email management policy and procedures
> - manage email that meets the definition of a government record in accordance with an approved retention schedule as per *The Archives and Public Records Management Act*
> - delete personal email and transitory records from the email system regularly
> - take appropriate precautions when sending email messages that contain personal or confidential information

[24] As a general rule, employees' government email accounts should not be used to store emails that are not official government records including personal emails. Providing employees with guidance on the proper management of email records will ensure emails that are official government records are regularly saved to the appropriate location in their filing system or electronic document management system and ensure email records are integrated with other records management practices, consistent with other records of the government institution. Once emails that are official government records are saved to the appropriate location, the copy in their email account can be deleted.

[25] Ensuring emails that are official government records are managed in a manner consistent with other records and filed in the appropriate locations may assist FOIP Coordinators when searching for responsive records. Additionally, if personal and transitory emails are regularly deleted, rather than being stored in their email accounts, it may reduce the number of emails that would need to be reviewed to determine if they are responsive. When an employee's employment with a government institution ceases, this would also limit the amount of work by other government employees saving emails to the appropriate locations

and sorting through personal emails that an employee has stored in their government email account.

[26] In the Information and Privacy Commissioner of Ontario resource, *Improving Access and Privacy with Records and Information Management*, it provides the following guidance:

> **Entry and Exit Protocols**
>
> Train staff on RIM [Records and Information Management] requirements when they join the institution. Ensure that all records are appropriately stored and managed before staff leave.
>
> As staff move between positions and institutions, it is easy for records to be lost, mishandled or destroyed inappropriately. Developing protocols for when staff start or leave positions can help prevent the loss of valuable information, as well as protect your institution from privacy breaches.
> …
>
> For staff exiting a position, it is important to ensure that records created or maintained during the individual's tenure are appropriately saved, securely destroyed or transferred to a replacement. Have the departing staff member verify that the following is completed prior to their last day:
>
> - Records have been stored, transferred to an archive or destroyed based on their retention schedules.
> - Personal non-work related information that may have been stored on a computer or in paper files has been destroyed.
> - Email records have been appropriately saved or destroyed.
>
> …
>
> Managers are responsible for ensuring that departing staff have completed all RIM requirements and should take steps to verify their completion.

[27] As a best practice, I encourage government institutions to have a documented practice in place to provide employees with the ability to gain access to any of their personal emails remaining in their government email account, within a specified timeframe of their employment ceasing (i.e. within 10-30 days of employment ceasing). This can assist the government institution to ensure it is not retaining any employee's personal emails where

there is no work related purpose and reduce the risk of privacy breaches resulting from the unnecessary retention of these records.

[28] Should the Applicant still have interest in gaining access to the personal emails detailed in this request, they could contact Environment to determine if the records can be accessed, if they still exist.

[29] I recommend that Central Services encourage government institutions to develop and implement a policy or procedure on the management of emails, including regularly saving email to appropriate locations and deleting personal or transitory emails.

IV FINDING

[30] I find that any emails sent or received by the Applicant constituting their personal emails, that are retained on the backup tapes, are not in the possession or control of Central Services for the purposes of FOIP.

V RECOMMENDATIONS

[31] I recommend that Central Services develop a policy or procedure to ensure access to information requests seeking emails from email backups are transferred to the appropriate government institution that may have the emails, if they still exist.

[32] I recommend that Central Services encourage government institutions to develop and implement a policy or procedure on the management of emails, including regularly saving emails to appropriate locations and deleting personal or transitory emails.

Dated at Regina, in the Province of Saskatchewan, this 17th day of March, 2020.

Ronald J. Kruzeniski, Q.C.
Saskatchewan Information and Privacy Commissioner