PROVINCIAL ARCHIVES OF SASKATCHEWAN

**Information Management Services**
**Effective Date: May, 2020**
**Last Revised: May, 2020**

# Guidelines for Records Management Outside of the Office

Regardless of the type of work environment (in office, in the field, or in alternative workspaces), government employees must practice good records and information management. When working anywhere outside of a traditional Government of Saskatchewan office space it is important for employees to ensure that all government (public) records they create or receive are managed appropriately, and that all necessary precautions to protect the security and confidentially of the records are taken.

Every government institution that allows its employees to work outside of the office must establish policies and procedures addressing information and records management that include the type of work that can be done, what records can leave the office, how records should be handled, security requirements for government records and devices, what access tools can be used by employees, etc.

These guidelines apply to all records regardless of their format made or received by Saskatchewan government institutions and offices subject to *The Archives and Public Records Management Act*.

## Complying with Legislation

There are several pieces of legislation that outline records management requirements in Saskatchewan including:

- *The Archives and Public Records Management Act*
- *The Freedom of Information and Privacy Protection Act*
- *The Health Information Protection Act*
- *The Electronic Information and Documents Act*

Government institutions also need to abide to records management requirements included in legislation specific to their institution.

Records that contain confidential or personal information require additional safeguards to ensure compliance with legislation. For more information, please reference relevant legislation on the Publications Saskatchewan website.

## Understanding Responsibilities

It is the responsibility of management at each government institution to ensure that work from home policies are in place. Management must also ensure compliance.

Records Management staff are responsible for the development and implementation of work from home policies, consulting with Information Technology staff to ensure electronic records are handled in a secure manner and for communicating any policy updates to employees.

Government employees are responsible for the following:

- Ensuring the security, integrity, and confidentiality of records for the entire time these records are outside of the office.
- Complying with their institution's work from home policies and security arrangements.

- Ensuring that complete records are captured, including associated metadata for electronic records.
- Organizing records in accordance with their institution's record management practices and if possible, with applicable records schedules.
- Ensuring records are available to other employees when needed.
- Preventing damage or destruction to government records. Disposal of government records requires the approval of the Provincial Archivist, and employees who wish to dispose of records must follow the disposal process as outlined in the Saskatchewan Records Disposal System: Guidelines to Records Disposal on the Provincial Archives' website.
- Immediately informing the appropriate individuals in the case of equipment, technology, or security failure in order to reduce data vulnerability or loss.

**Best Practices**

It is recommended that employees use a government device, VPN, and remote desktop in tandem for optimal record security of government records when working outside the office. The following are some best practices:

1. **Using a Secure Government Device (e.g. a laptop, tablet, or cellphone)**
   When using one of these devices it is preferable to save documents to a government drive through a secure connection. If this is not possible, documents can be saved to the device's desktop or a secure government USB. It is important to ensure records are named and organized in a way that is consistent with the institution's records management requirements for ease of transfer to the institution's internal records keeping system (e.g. the respective government drive) at the earliest opportunity. There should be no copy of the records left on the device. When using one of these devices an employee should not share their password or access to the device, and should not use it for personal purposes. When not in use these devices should be secured and safely stored, preferably out of sight to minimize risk of theft.

2. **Using a VPN (Virtual Private Network)**
   When working out of the office it is imperative that a secure connection using a VPN is provided to employees for saving and accessing records on government drives or networks. While it is recommended to use a government device, if a personal device is used by a government employee, the device should be secured in accordance with government standards.

3. **Using a Remote Desktop**

   Some employees may have the option of using a remote desktop which allows them to access their work computer and drives from another device, with minimal disruption to regular recordkeeping practices. Employees should access this service from a secure device compliant with government standards and disconnect when access is not required.

**4. Paper Files**

It is recommended that government records are not removed from an office space or designated records storage. When possible, convenience copies should be used for reference rather than removing the official record.

If an institution allows its records to be removed from its sites, it must have strict procedures regarding this process. If this occurs, it is important to ensure that:

- A log is maintained that tracks the location of records and identifies the employees responsible for the records' temporary custody.
- Verification of record integrity and completeness occurs upon return.
- Required internal authorization has been received.
- Only the minimum amount of records needed are removed from the office.
- If possible records are printed using printers on a government network. Documents that are modified or created outside of the office should be kept secure until they can be properly printed and filed in the institution's recordkeeping system. If this is not possible, employees will need to ensure that:
    - Printers used are secure and that they are cleared of the government data immediately.
    - The printed records are securely retained until they are brought back to the office and filed in accordance the institution's practices.

**5. Transitory records**

Transitory records are either physical or digital records that have only a short term value, are needed to complete a routine task, or are exact copies of official records made for ease of reference. Examples of transitory records are convenience copies, drafts with formatting changes, etc. Any transitory records created/received while working out of office, should be destroyed by employees as soon as possible when no longer needed and in compliance with their institutions' policies and applicable safeguards. For more information about transitory records please refer to "Guidelines for the Management of Transitory Records" found on the Provincial Archives of Saskatchewan website: https://www.saskarchives.com/sites/default/files/pdf/transitory_rec_guide_fin.pdf.

**6. Emails, Texts and Instant Messaging**

While working outside of the office many employees may be inclined to use these systems of communication more regularly. All employees should remember that if these messages are made in the course of their work and are related to decision making, policy and procedures, or operations and services, these messages are government records and need to be treated as such. Emails, texts and instant messages that are government records must be captured and managed in the institutions' records keeping systems. It is recommended to keep clear separation between work and personal messages, preferably using government devices and accounts only for government business.

7. **Personal Devices**

   It is highly recommended that personal devices are not used for government business. If personal devices are used, they need to be secured to government standards. Government records or their copies should not be saved or maintained on personal devices. They should be kept separate within the system from personal records and should be transferred to the appropriate internal institutional records keeping system as soon as possible along with all copies.

8. **Data Security**

   Threats to information security are always present and need to be protected against. Employees are reminded to:

   - Not reply to or click links/attachments in emails, texts, etc. from unknown sources.
   - Never give out passwords, pins, or other security codes.
   - Check for suspicious content, addresses, or subjects in the emails.
   - If an email, text, etc. seems suspicious but an employee cannot determine for themselves, they should verify by contacting (using a different method of contact like a phone) the sender or check with their institutions IT services.
   - Delete phishing and other scam emails, do not reply or unsubscribe.

   For more information go to the IT Security Services page in Taskroom or consult your IT Security team.

**References:**

Saskatchewan Records Disposal System: Guideline to Records Disposal

https://www.saskarchives.com/sites/default/files/pdf/rds_update_sept2015.pdf

Glossary of records management terms:
https://www.saskarchives.com/sites/default/files/pdf/glossaryofrmterms_v.02_2017.pdf

Government of Saskatchewan “Working from Home – Technology & Access Guide”:https://taskroom.sp.saskatchewan.ca/Documents/Working-from-Home-Technology-and-Access.pdf

Government Standards: “Information Security Policy”:
https://taskroom.sp.saskatchewan.ca/Documents/Mobile-Wireless-Devices-Policy.pdf

IT Security Services:

https://taskroom.sp.saskatchewan.ca/how-do-i/get-it-support/it-security