



Information Management Handbook

A management and employee guide to access, privacy, security, retention, disposal and overall management of records in government and local authorities in Saskatchewan.



confidential

for the Govt

Contents

- 3 Introduction**
- 6 Introduction to the Access and Privacy Section**
- 7 Access to Records
- 8 Privacy
- 10 Privacy Rules and Principles
- 12 Personal Health Information
- 13 Information and Privacy Commissioner
- 15 Introduction to Safeguarding Information**
- 16 Computers
- 16 Passwords
- 17 Mobile Devices
- 19 E-Mail
- 19 Information Technology Acceptable Usage Policy
- 21 Introduction to Records Management, Retention and Disposal**
- 21 Records Management and Retention of Records
- 23 Disposal of Records
- 24 Securely Destroying Records Approved for Disposal, Computers, Mobile Devices and Other Hardware
- 27 Privacy and Security Incidents**
- 29 Resources**



Introduction

Do you ever wonder?

Are there rules regarding the information on my computer or for paper records in my desk drawer? Can I share this information with anyone? Can I shred my records when I no longer need them? Is it okay to share my password with my colleagues?

These are some of the many questions that employees encounter over the course of a career in government or in a local authority. This handbook provides you with answers to some of those questions.

What the handbook will tell you

The handbook provides information about rules and best practices related to the collection, use, disclosure, public access, protection, retention and disposition of records in your possession or control.

The handbook also provides reference and contact information, so when you have more detailed or specific questions, you will know where to turn.

To whom does the information in the handbook apply?

The handbook is applicable to all employees in government institutions or local authorities in Saskatchewan.

The handbook was prepared by

This handbook is a reference tool which was prepared by the Ministry of Justice and Attorney General, with support from the Information Technology Division, Provincial Archives of Saskatchewan, Ministry of Central Services, Ministry of Health, Ministry of Education, Ministry of Advanced Education, Ministry of Government Relations and the Public Service Commission.

This handbook is for informational purposes only. Applicable law and policy should be consulted for a more detailed reference.

For more information, see the Resources section at the back of this handbook.

What is a record?

This handbook relates to information and records in the possession or under the control of government institutions or local authorities in Saskatchewan.

The Freedom of Information and Protection of Privacy Act, The Local Authority Freedom of Information and Protection of Privacy Act, The Health Information Protection Act and The Archives and Public Records Management Act all have the same definition of a record, which is:

“record” means a record of information in any form and includes information that is written, photographed, recorded or stored in any manner, but does not include a computer program or other mechanism that produces records;

Records include:

documents, draft documents, journals, spreadsheets, maps, drawings, photographs, letters, vouchers, paper, electronic and digital records, video, text messages, e-mail, contents of an electronic database and all other instances of recorded information in your work environment.

What is information?

Information is what a record contains. It is also a term often used to refer to the content of electronic databases or applications. Regardless of the form, all information recorded and in the possession or control of a government institution or local authority is a record subject to one or more of the Acts above.

For more information, see the Resources section at the back of this handbook.

CONFIDENTIAL

Introduction to the Access and Privacy Section

Government institutions and local authorities in Saskatchewan are all subject to one or more of the following access and privacy laws.

Government Institutions

Government ministries, Crown corporations, boards, commissions and other agencies of Executive Government listed in the regulations are subject to:

- [The Freedom of Information and Protection of Privacy Act](#); and
- [The Health Information Protection Act](#)

Local Authorities

Most local authorities, including municipal governments, school boards, post-secondary institutions and library boards, are subject to:

- [The Local Authority Freedom of Information and Protection of Privacy Act](#)

The Saskatchewan Health Authority, special care homes and other local authorities designated as trustees under *The Health Information Protection Act* are subject to:

- [The Local Authority Freedom of Information and Protection of Privacy Act](#); and
- [The Health Information Protection Act](#)

Health Trustees

The Health Information Protection Act applies to organizations and individuals defined as “trustees” in the Act. These include government institutions and certain local authorities in the health sector, but also include personal care homes, mental health facilities, medical laboratories, pharmacies, community clinics, the Saskatchewan Cancer Agency, ambulance operators, regulated health professions and health profession regulatory bodies (except where operated by a local authority). Trustees in this category are subject to:

- [The Health Information Protection Act](#)

For more information, see the Resources section at the back of this handbook.

Want to learn more?

Read the definitions of “government institution,” “local authority” and “trustee” in section 2 of the respective Acts if you are uncertain where you fit.

To download a copy of Acts or Regulations in Saskatchewan, including the statutes mentioned above, please visit the [Publications Saskatchewan](#) website.

Access to Records

A Right to Access Records

The Freedom of Information and Protection of Privacy Act gives any person the right to access records in the possession or under the control of a government institution in Saskatchewan.

The Local Authority Freedom of Information and Protection of Privacy Act gives the same right of access to records in the possession or under the control of a local authority.

The Health Information Protection Act provides a right of access to individuals to their own personal health information in the custody or control of a trustee. See page 12 for more information.

How the process works

Individuals complete an [Access to Information Request Form](#), available online and in many government offices.

Once a request is received, the government institution or local authority has 30 days to respond. In most workplaces, an Access Coordinator (sometimes called a FOIP Coordinator) will prepare a response, including reviewing the records to ensure all mandatory and discretionary exemptions are addressed.

For more information, see the Resources section at the back of this handbook.

What gets disclosed?

The Acts give a right of access to any record; however, certain information may be exempt from release. The Acts provide a balance between access and confidentiality and include both mandatory and discretionary exemptions from disclosure. Some examples include records that disclose a confidence of Cabinet, certain third party information, records subject to solicitor-client privilege and personal information.

Roles and Responsibilities

Your workplace has someone assigned to manage this process. Find out who this is and make sure you cooperate when an access request arrives. Remember, the law requires a response.

Resources and Training

Access to information and protection of privacy resources, including a number of general resources and an online training tool, are available at the links below:

- [Access Resources](#)
- [Privacy Resources](#)
- [General Resources](#)
- [Online Training](#)

Privacy

The privacy of personal information in the possession or under the control of a provincial government institution is protected by *The Freedom of Information and Protection of Privacy Act*.

For local authorities, personal information is protected by *The Local Authority Freedom of Information and Protection of Privacy Act*.

The personal health information in government institutions and certain local authorities is governed by *The Health Information Protection Act*. See page 12 for more information.

For more information, see the Resources section at the back of this handbook.

What is personal information?

Personal information is defined in both *The Freedom of Information and Protection of Privacy Act* and *The Local Authority Freedom of Information and Protection of Privacy Act* and includes just about any personal information about an identifiable individual. For example, it may include information about race, religion, family status, age, place of origin, employment or criminal history, financial information, address and telephone number, the views or opinions of someone about that person, along with a host of other information.

How is personal information protected?

The legislation includes rules on:

- Consent;
- Collection, use and disclosure;
- Informing individuals about the purpose for collection;
- Accuracy of personal information; and
- The right to access and request corrections.

These rules must be followed at all times.

Refer to the grids on the following pages for additional information.

For more information, see the Resources section at the back of this handbook.

Privacy Rules and Principles

Collection and Purpose

- Government institutions can only collect personal information for programs or activities that is consistent with their mandate.
- Collection shall be limited to only what is needed for a specific purpose.
- Individuals should be informed of the purpose of collection (this is a requirement when collecting directly from them).

Use and Disclosure

Personal information can be used or disclosed:

- For the purpose the information was collected;
- With consent; or
- Where allowed by *The Freedom of Information and Protection of Privacy Act*.

Retention

- Personal information should only be retained as long as necessary to serve the purpose for which it was collected, or as specified by law.
- Follow *The Archives and Public Records Management Act* when disposing of records.

Safeguards

Appropriate safeguards are needed to ensure the safety of personal information.

Safeguards may be:

- Administrative (policies or codes);
- Physical (locks or safe storage);
- Technical (firewalls or encryption).

For more information, see the Resources section at the back of this handbook.

Right to Access and Right of Correction

- Individuals have the right to access their own personal information, subject to certain restrictions.
- Individuals can request a correction to personal information held in government records.

Consent

- While consent is not always necessary to use or disclose personal information, it is a best practice that should be considered.
- Where consent is required by *The Freedom of Information and Protection of Privacy Act*, it should be in writing.

Accountability

- Each government institution is accountable for the personal information in its possession or under its control.
- Each government institution has a Privacy Officer.

Openness and Compliance

- Policies and procedures should be made available to the public.
- Individuals should be able to challenge a government institution's handling of their personal information.

This is based on *The Freedom of Information and Protection of Privacy Act* and *The Overarching Personal Information Privacy Framework for Executive Government* available at <https://publications.saskatchewan.ca:443/api/v1/products/79817/formats/90907/download>. Similar rules and principles will apply in local authorities.

For more information, see the Resources section at the back of this handbook.

Personal Health Information

The Health Information Protection Act (HIPA) provides rules and guidelines that govern the collection, use and disclosure of personal health information in Saskatchewan.

What is personal health information?

Personal health information is defined in the Act to include information about the health of an individual or health services that have been provided to an individual. Examples include a patient record held by a hospital, registration information held by the Ministry of Health to register individuals for insured services, and records containing personal health information held by government institutions, including employee personnel files.

HIPA applies to whom?

HIPA applies to “trustees,” including:

- Government institutions subject to *The Freedom of Information and Protection of Privacy Act*; and
- All key stakeholders in the health system, including the Saskatchewan Health Authority and affiliates, special care homes, personal care homes, mental health facilities, laboratories, pharmacies, community clinics, the Saskatchewan Cancer Agency, ambulance operators, regulated health professions and health profession regulatory bodies.

The Act does not apply to local authorities outside the health sector.

What are the rules?

HIPA places duties or responsibilities on trustees (organizations and individuals subject to the Act) to protect the privacy of personal health information. For example:

- Trustees should only collect, use or disclose personal health information required to provide a service;
- The primary purpose for collecting personal health information must be for the benefit of the individual;
- Trustees must protect personal health information.

For more information, see the Resources section at the back of this handbook.

The Act identifies certain rights of individuals, including:

- The right to consent to the use and disclosure of personal health information, except as otherwise authorized by the Act;
- The right to access records about themselves.

For more information, contact the Ministry of Health by phone at 1-800-667-7766 or by email at health.infoprivacy&accesshelp@health.gov.sk.ca.

Information and Privacy Commissioner

The Saskatchewan Information and Privacy Commissioner is an independent officer of the Legislative Assembly with oversight powers over *The Freedom of Information and Protection of Privacy Act*, *The Local Authority Freedom of Information and Protection of Privacy Act* and *The Health Information Protection Act*.

The Commissioner:

- Conducts reviews and makes recommendations regarding access requests made under any of these statutes;
- Investigates privacy incidents and complaints;
- Conducts public education on access and privacy issues; and
- Reports annually to the Legislative Assembly.

Further information about the Information and Privacy Commissioner is available at the Commissioner's web site at: www.oipc.sk.ca

Note: Government and local authority managers and employees with questions about access and privacy should consult their internal access and privacy officials or the Access and Privacy Branch, Integrated Justice Services, prior to contacting the Information and Privacy Commissioner. Most questions can be handled internally.

For more information, see the Resources section at the back of this handbook.



Introduction to Safeguarding Information

Safeguards must be in place to protect information from loss, theft or unauthorized access, use, copying, modification or disclosure. This is especially important for sensitive and confidential information such as personal information or personal health information.

Different types of information may require different levels of protection. For example, brochures and pamphlets for distribution to the public may require no special protection at all; whereas sensitive Cabinet documents or records containing personal health information will require high levels of protection.

Your workplace may have an information security classification scheme in place (e.g. labeling records confidential, restricted, public, etc.) to help determine appropriate levels of security. If so, find out how it should be applied.

Safeguards exist in many forms, including administrative, physical and technical.

Examples of administrative safeguards include:

- A requirement for security clearance to enter certain office areas or where confidential records are stored;
- Policies and procedures that limit access to personal information on a need-to-know basis.

Examples of physical safeguards include:

- Locks on filing cabinets;
- Doors, locks, etc. restricting access to offices, records storage areas, rooms containing computers or other devices, etc.

Examples of technical safeguards include:

- Firewalls on computer networks;
- The use of encryption to prevent unauthorized access to information on laptops and other mobile devices.

You have a role to play. Know the safeguards required in your work place.

The following pages provide guidance on what you can do to protect important records.

For more information, see the Resources section at the back of this handbook.

Computers

Computers are a vital part of today's work environment. Care must be taken to protect computers and their networks, not only as assets, but also because lack of care puts records and information at risk.

- Follow all IT policies in effect in your workplace. For example:
 - Do not install software or disable any element of the standard configuration, including encryption, screen savers, passwords or antivirus software;
 - Ensure proper operation of antivirus and spam software;
 - Use computers for business purposes only;
 - Check all files for malicious content before loading or using them.
- Be aware of acceptable use of technology policies in effect in your workplace.

Passwords

Passwords are the first line of defence in protecting information. Passwords protect voice mail, information stored on the network, databases, mobile devices and elsewhere. Below are some tips to using passwords:

- Create strong (hard-to-guess) password;
- Do not share your password with anyone;
- Change your password immediately if you suspect someone knows it;
- Do not write password down or save them to file;
- Select different password for business and personal use.

To construct a hard-to-guess password, use:

- Six to eight characters or more;
 - Alpha-numeric characters;
 - Special characters;
 - Upper and lower case letters; and
 - Non-dictionary words.
- (Requirements may vary in different work environments.)

Try the following, but do not use this as your password:

- Think of a phrase like "the rain in Spain falls mainly on the plain";
- Take the first letter from each word in your phrase: trisfmoTp.

For more information, see the Resources section at the back of this handbook.

Add complexity:

- Substitute numeric characters for letters: *tr1sfmotp*
- Insert special characters: *tr1\$fmotp*
- Add upper case letters: *Tr1\$fmotP*

Mobile Devices

Mobile devices include laptops, cell phones and removable media, such as CD's or USB flash drives, among other things. In short, any electronic mobile device that can send, receive or store information.

Each new generation of technology brings increased storage capacity, added convenience and usability. However, it may also introduce new or additional risks to privacy, confidentiality, availability and integrity of the information stored on those devices.

Think about the information stored on the device:

- If possible, do not store sensitive or personal information on mobile devices. If you must do so, then store only what is necessary and delete the information from the device as soon as possible;
- Backup the files stored on the device to the network;
- Use separate mobile devices for personal and business purposes;
- Know what information is stored on these devices (this will be important if you lose them).

Administrative, Physical and Technical Safeguards

Mobile devices should be kept secure to protect the device itself and also, to protect the information stored on it. Consider the following:

- If possible, physically secure the device. Consider securing a laptop with a cable locking device;
- Avoid leaving the device unattended. If you must do so, consider placing it in a locked cabinet or shield it from view;
- Instead of carrying a USB flash drive with you, store it in a locked cabinet when not in use;
- Do not share the device with others;
- Use the password protection feature of cell phones, laptops and all mobile devices and use a hard-to-guess password;

For more information, see the Resources section at the back of this handbook.

- Log off the network and/or applications at the end of a shift or when leaving the office for extended periods of time;
- Consider encryption for USB flash drives, laptops and other mobile devices.

Report Incidents

- If the mobile device is lost or stolen, report it to your supervisor, privacy or security officer or your IT service provider as soon as possible;
- If you find a mobile device, report it to your supervisor, privacy or security officer or your IT service provider and do not connect it to the network.

When Traveling

There are some additional risks when traveling. Consider the following:

- Laptops should not be left unattended in vehicles, unless absolutely necessary;
- If left in a vehicle, place it inside the locked trunk or shielded from view;
- Laptops are carry-on luggage; do not check as baggage;
- Lock the laptop in the hotel room safe, if available. If not available, consider using a locking cable to secure the laptop to a device that is too heavy to move or shield the laptop from view by storing it in a closet or drawer.

Wireless Internet (Wifi)

If you use wireless internet, there may be additional risks. Consider the following:

- Use only approved wireless equipment;
- Use a VPN (virtual private network) whenever possible to encrypt your information transmissions;
- Turn off shared folders;
- Keep security and service patches up-to-date;
- Keep firewall, virus protection and spam or spyware up-to-date;
- Configure your laptop to not automatically connect to any available network;
- Never disclose wireless encryption details to anyone, including family members;
- Before connecting to a wifi network, confirm that it is a valid network;
- Shut off your wireless card when you are not using it;

For more information, see the Resources section at the back of this handbook.

- Be cautious about your computer activities in public locations;
- Do not access sensitive organizational data over a wireless connection, except through a VPN.

E-Mail

E-mail is an essential tool in today's work environment. The majority of written communications within the office and beyond takes place using e-mail. Precautions should be taken when considering sending personal or confidential information using e-mail.

Personal and confidential information should not be forwarded using e-mail, unless there is a valid business need and unless the following precautions have been taken:

- Consider whether it is necessary to send any personal or confidential information in order to carry out the task. Do not include it if it is not needed;
- If some personal or confidential information must be sent, provide only the minimal amount necessary for the purpose and consider whether the message can be anonymized or sent using de-identified information (e.g. name, address, telephone number, Health Services Number, etc. are removed or encrypted);
- Limit the distribution of the information to only those recipients who have a legitimate need to know the information;
- Include a confidentiality notice on all e-mail messages;
- Verify the address you are sending to before hitting the SEND button.

Information Technology Acceptable Usage Policy

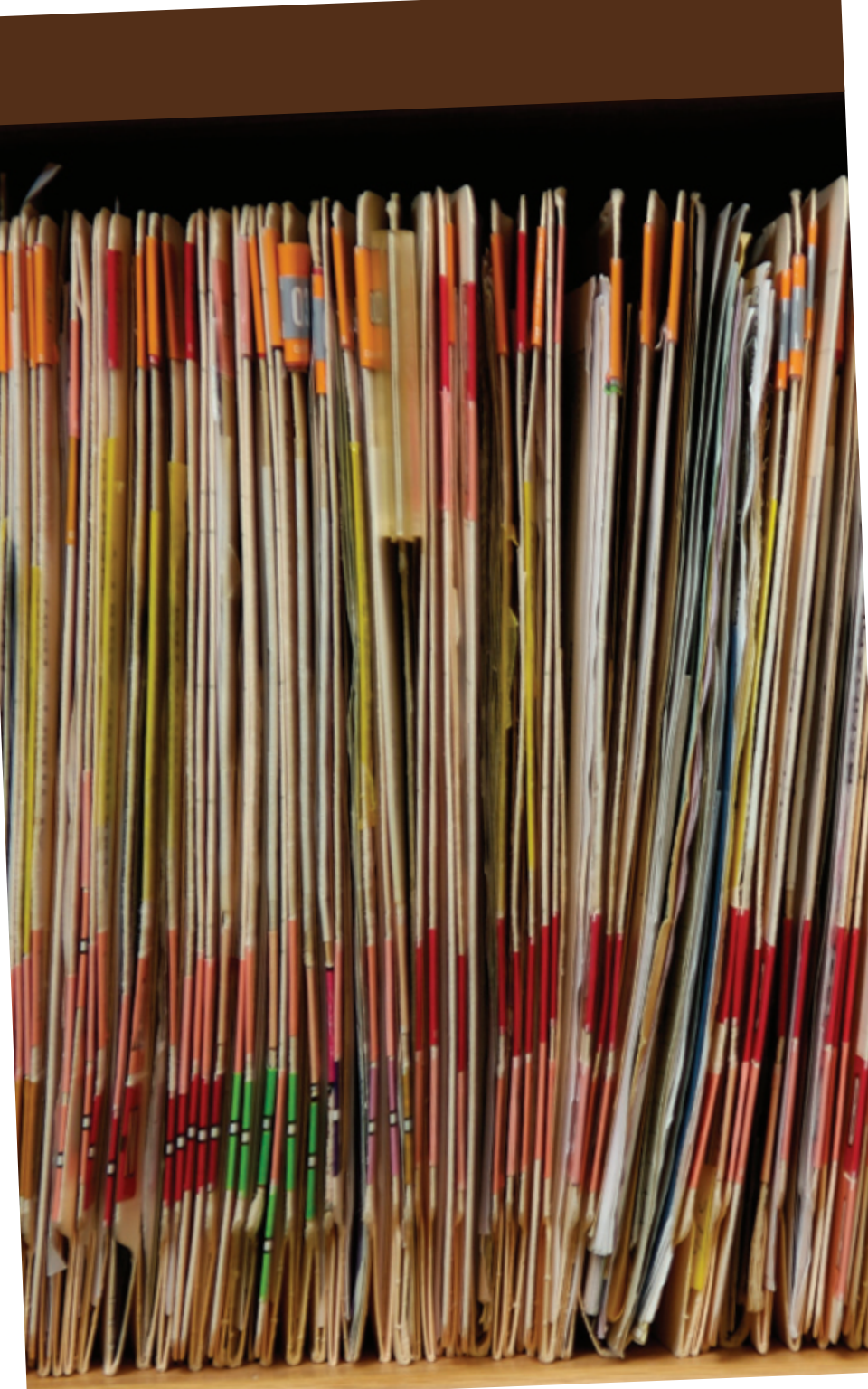
In Government

The *Information Technology Acceptable Usage Policy* sets policy and guidelines for government employees using e-mail and all other forms of technology. Become familiar with what is acceptable and what is not.

In Local Authorities

Local authorities may have a similar acceptable use policy. Become familiar with the rules in your workplace.

For more information, see the Resources section at the back of this handbook.



Introduction to Records Management, Retention and Disposal

Records are the “institutional memory” of your organization; they are necessary for decision making, policy development, program implementation and for almost every aspect of day-to-day office work.

Records should be organized, retained for an appropriate length of time and disposed of in a safe and secure manner. Remember (from the discussion on page 4) that records include not just paper, but also electronic records, e-mail, and many other things.

Learn more on the following pages about records management and retention and disposal of records.

Records Management and Retention of Records

Records classification and retention schedules are the foundation of an effective records management program. Schedules are used to classify and manage records while they are being used in daily activities. They help to organize and retain records, while also providing guidance on how long each record should be retained.

For more information, see the Resources section at the back of this handbook.

In Government

The Archives and Public Records Management Act governs the retention and disposal of records in government. The Act gives the Provincial Archivist the authority to approve the disposal of public records in Saskatchewan. Records in government must be retained in accordance with one of the following:

Administrative Records Management System 2014 (ARMS2014):

- A combined records classification system and retention schedule;
- For use by all government institutions for administrative records, including management of facilities, property, material, finance, human resources and information systems.

Operational Records System (ORS):

- A classification system and retention schedule for the operational records of an organization. Designed to be compatible with ARMS2014;
- Unique to each organization and documents the mandated functions of your government institution;
- Usually consists of client files, program files and subject files.

Collectively, ARMS2014 and ORS will help you manage your active files, while at the same time ensuring you retain the records for an appropriate length of time.

For more information about records management in government, refer to the *Saskatchewan Records Management Policy*, the *Saskatchewan Records Management Guidelines*, the *Saskatchewan E-mail Management Guidelines*, and other resources on the Provincial Archives of Saskatchewan website: www.saskarchives.com

For more information, see the Resources section at the back of this handbook.

What about local authorities?

Local authorities will follow the same basic rules, although they may not be subject to *The Archives and Public Records Management Act*. There may be specific records classification systems and retention schedules in effect in your workplace – get to know them. For example:

- Local authorities in the health sector should be aware of retention policies that apply to their records. In particular, *The Health Information Protection Act* addresses the retention of personal health information;
- School divisions follow the “Records Retention and Disposal Guide for Saskatchewan School Divisions (December, 2012)”;
- Municipalities should consult approved retention schedules or contact the Ministry of Government Relations for additional information.

Disposal of Records

At some point in time, most records will cease to be worth keeping in your office. Can they simply be thrown away? No they cannot.

Inappropriate disposal of records can result in privacy incidents (client or patient files in a recycling bin), security incidents (confidential security documents not removed from a hard drive of a salvaged computer) and other undesirable results. Care must be taken to properly dispose of records.

For more information, see the Resources section at the back of this handbook.

The Process in Government

Government records must be disposed of in accordance with *The Archives and Public Records Management Act*. The Provincial Archives of Saskatchewan manages and administers the Records Disposition System which does the following:

- Provides for a review to confirm that records are related to ARMS2014 or to an appropriate ORS schedule and that the required retention periods have been met;
- If the records are eligible for disposal, they are reviewed by an appraisal archivist;
- Records of continuing historical value are acquired and preserved by the Provincial Archives of Saskatchewan;
- Where records have no historical value, written authority is given to proceed with secure destruction.

For more information about records retention and disposal in government, visit the Provincial Archives of Saskatchewan website at:

www.saskarchives.com

In Local Authorities

Similar policies may be in effect in local authorities.

Securely Destroying Records Approved for Disposal, Computers, Mobile Devices and Other Hardware

Once records are approved for disposal, care must still be taken.

Paper Records

Paper records containing personal information or confidential information must never be recycled. A secure method of disposal must be used. For example, use internal crosscut shredding or have a contract with a qualified, secure shredding service.

For more information, see the Resources section at the back of this handbook.

What about electronic records?

Personal and sensitive information may be found on a range of electronic storage media devices, including computers, cell phones, fax machines, photocopiers and printers, as well as portable/removable storage devices such as CDs, DVDs and USB drives. Information must be removed (not just deleted) from these devices before they go out of service.

Within Government

All permanent storage media must be removed from government-owned equipment before it is transferred outside of the government or disposed of by any other means.

Storage media being transferred within the government must have all data removed using a secure media eraser.

The Information Technology Division (ITD), Ministry of Central Services, will ensure the storage media on ITD-leased computers is thoroughly cleansed before it is returned at the end of the lease.

For other equipment, arrangements can be made to remove all information from the permanent storage media using a secure media eraser.

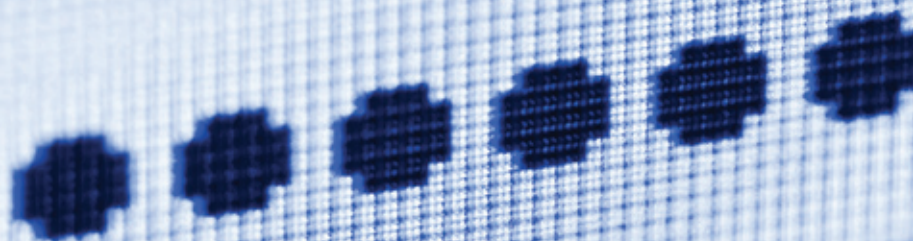
If the permanent storage media cannot be sanitized, arrangements must be made for the destruction of the storage media.

In Local Authorities

Similar policies may be in effect in local authorities.

For more information, see the Resources section at the back of this handbook.

Login



Login

Privacy and Security Incidents

Despite best efforts, there may come a time when you have a privacy breach or a security breach. What do you do then?

A Privacy Breach

- The Access and Privacy Branch, Integrated Justice Services, has established *Privacy Breach Management Guidelines* with recommendations for what to do in the event of a confirmed or potential breach of privacy;
- Your workplace may have its own guidelines in place;
- In the event of a suspected breach, the first step is always to notify your supervisor and the Privacy Officer (or equivalent) for your workplace.

A Security Breach

- In the event of a security incident involving government information resources such as computers and databases, you should immediately notify your supervisor and the Privacy Officer/ Security Officer (or equivalent).

Privacy and security officials will work together, as necessary, to contain and manage incidents.

For More Information

Please contact your institution's Privacy Officer for the protocol in your workplace.

View the *Privacy Breach Management Guidelines* when responding to incidents involving the improper collection, use or disclosure of personal information or personal health information.

Additional information about privacy breach management can also be found on the website of the Office of the Information and Privacy Commissioner: www.oipc.sk.ca

For more information, see the Resources section at the back of this handbook.



Info

Resources

Internal

If you have questions or want more information, the best place to start is within your own workplace. You may have any or all of the following positions that can help:

- Access and Privacy Officers/ FOIP Coordinators

Each government institution will have its own Access and Privacy Officer or FOIP Coordinator. This is your first point of contact for access and privacy issues or questions. For a listing of the access and privacy officials in each government institution, visit the [government institution contact list](#). Local authorities may also have a designated individual for these positions.

- IT Administrators/ Security Officers

For questions regarding IT administration, security and IT policy, check with your information technology area.

- Records Manager

For questions about classification of records, retention and disposal of records, contact your Records Manager, often located in a central administration office.

For additional help

- Access and Privacy Branch, Integrated Justice Services

The Access and Privacy Branch provides advice and support to government institutions and local authorities subject to *The Freedom of Information and Protection of Privacy Act* and *The Local Authority Freedom of Information and Protection of Privacy Act*.

Resources and online training to help manage access to information and privacy issues within government institutions in Saskatchewan can be found here:

[Access Resources](#)
[Privacy Resources](#)
[General Resources](#)
[Online Training](#)

- **Information Technology Division**, Ministry of Central Services

ITD provides information technology services for much of government.

- **Ministry of Advanced Education**

Universities, colleges and other post-secondary institutions in Saskatchewan can contact Advanced Education with specific questions about practices in this sector.

- **Ministry of Education**

School divisions and libraries can contact Education with specific questions about practices in this sector.

- **Ministry of Central Services**

Central Services manages salvage and storage operations for the government, including providing secure records storage for many government records no longer in active use and managing the salvage of government equipment.

- **Ministry of Health**

For information about *The Health Information Protection Act*, contact the Ministry of Health using one of the following methods:

Ministry of Health toll-free inquiry line: 1-800-667-7766

E-mail: health.infoprivacy@accesshelp@health.gov.sk.ca

Website:

<https://www.saskatchewan.ca/residents/health/accessing-health-care-services/your-personal-health-information-and-privacy>

- **Ministry of Government Relations**

Government Relations provides advice on practices in the municipal sector.

- **Office of the Information and Privacy Commissioner**

The Information and Privacy Commissioner is an independent officer of the Saskatchewan Legislative Assembly. The Commissioner provides oversight for *The Freedom of Information and Protection of Privacy Act*, *The Local Authority Freedom of Information and Protection of Privacy Act* and *The Health Information Protection Act*.

- **Publications Saskatchewan**

Publications Saskatchewan publishes and distributes legislation, regulations and other government publications on behalf of the Government of Saskatchewan.

- **Provincial Archives of Saskatchewan**

Records management, retention and disposal practices for government are managed by the Provincial Archives of Saskatchewan.



Contact: