Contact:

8M/10/09

Saskatchewan
Ministry of
Justice and
Attorney General

# 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

# Contents


APR
04
MAR
04
R
O
B
R
I
S
R
I
V

# Introduction

**Do you ever wonder?**

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 OK to share my password with my colleagues?

These are some of the many questions that sooner or later most 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 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 or local authorities in Saskatchewan.

**The handbook was prepared by**

This handbook is a reference tool prepared by the Ministry of Justice and Attorney General with support from the Information Technology Office, Saskatchewan Archives Board, Ministry of Government Services, Ministry of Health, Ministry of Education, Ministry of Advanced Education, Employment and Labour, Public Service Commission, and Ministry of Municipal Affairs.

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

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

## What is a record?

All the information in this handbook is about information and records in the possession or under the control of government institutions and local authorities in Saskatchewan.

*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* all have the same definition, which is:

> *"record" means a record of information in any form and includes information that is written, photographed, recorded, digitized or stored in any manner, but does not include computer programs or other mechanisms that produce records;*

It includes:

> word processed documents, draft documents, journals, spreadsheets, maps, drawings, photographs, letters, vouchers, paper records, electronic records, optical or digital records, 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, and 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*.

Regional health authorities, special care homes and other local authorities designated as trustees in *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 Queen's Printer website at www.qp.gov.sk.ca

## 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 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 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 in many government offices and on the Internet at Queen's Printer (www.qp.gov.sk.ca). Once a request is received the government institution or local authority has only 30 days to respond. In most workplaces, an access coordinator (sometimes called a Privacy Officer or 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. 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

Additional resources and training on access and privacy in government and local authorities including easy-to-use, on-line courses are available at: www.justice.gov.sk.ca/accessandprivacy

## Privacy

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

The privacy of personal information in the possession or control of a local authority is protected by *The Local Authority Freedom of Information and Protection of Privacy Act*.

The personal health information in government 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 laws have rules about:

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

These rules must be followed at all times!

Refer to the grid on the following page for additional information.

**Resources and training**

Additional resources and training on access and privacy in government and local authorities including easy-to-use, on-line courses are available at: www.justice.gov.sk.ca/accessandprivacy

*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 consistant with their mandate.
- Collection shall be limited to only what is needed for a purpose.
- Individuals should be informed of the purpose for collection (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 in law.
- Follow *The Archives Act, 2004* when disposing of records.

### Safeguards

Appropriate safeguards are needed to ensure safety of personal information. Safeguards may be:

- Administrative (policies, codes).
- Physical (locks, safe storage).
- Technical (firewalls, 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 correction to personal information 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 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.

Based on *The Freedom of Information and Protection of Privacy Act* and *The Overarching Personal Information Privacy Framework for Executive Government* available at www.justice.gov.sk.ca/accessandprivacy

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 received by 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 with personal health information held by a government institution including many 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 regional health authorities 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 about *The Health Information Protection Act* check the Ministry of Health website at:
www.health.gov.sk.ca/health-information-protection-act
or call 1-800-667-7766 or e-mail HIPAFOIhelp@health.gov.sk.ca.

## Information and Privacy Commissioner

The Office of the Information and Privacy Commissioner of Saskatchewan is an independent office 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.
- Reports annually to the Legislative Assembly.

Further information about the Office of 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 of the Ministry of Justice and Attorney General before 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.*


F8
F9
F10
&
*
(
9
Y
U
O
H
N
<
,

# Introduction to Safeguarding Information

Safeguards must be in place to protect information from loss or 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 records containing personal health information or sensitive Cabinet documents 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 certain office areas or confidential records.
- 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, computer rooms, 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 the records and information at risk.

- Follow all IT policies in effect in your workplace:
  - Don't install software or disable any element of the standard configuration including encryption, screen saver 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 the file.
- 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 networks, databases, mobile devices, and elsewhere. Passwords need to be taken very seriously and not dismissed as an annoyance.

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

**Constructing a "hard-to-guess" password:**

- Use:
  1. Six to eight characters or more;
  2. Alphanumeric characters;
  3. Special characters;
  4. Upper and lower case letters; and
  5. Non-dictionary words.

  (Requirements may vary in different work environments.)

Try the following (but don't use this as your password):

- Think of a phrase like: "*The rain in Spain falls mainly on the plain*".
- Take the 1st character from each word in your phrase: *trisfmotp*

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

- Add complexity:
  *a.* Substitute numeric characters for letters: *tr**1**sfmotp*
  *b.* Insert special characters: *tr1**$**fmotp*
  *c.* Upper case letters: ***T**r1$fmot**P***

## Mobile Devices

Mobile devices include laptops, Personal Digital Assistants (PDAs), cell phones, BlackBerries, MP3 players, removable media such as CD's or USB flash drives (sometimes called 'memory' or 'thumb' 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. Safeguards are needed!

### Think about the information stored on the device

- Do not store sensitive or personal information on mobile devices if possible. 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:

- Physically secure the device if possible. 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, BlackBerries, laptops and all mobile devices – 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, your security or privacy officer or your IT service delivery 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 for one person to move or shield the laptop from view by storing it in a closet or drawer.

**Wireless internet**

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, spam/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.
- Don't access sensitive organizational data over wireless except through a VPN.

## E-Mail

E-mail is an essential tool in today's work environment. A significant amount, perhaps 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 (i.e., 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(es) you are sending to before hitting the SEND button.

## Information Technology Acceptable Usage Policy

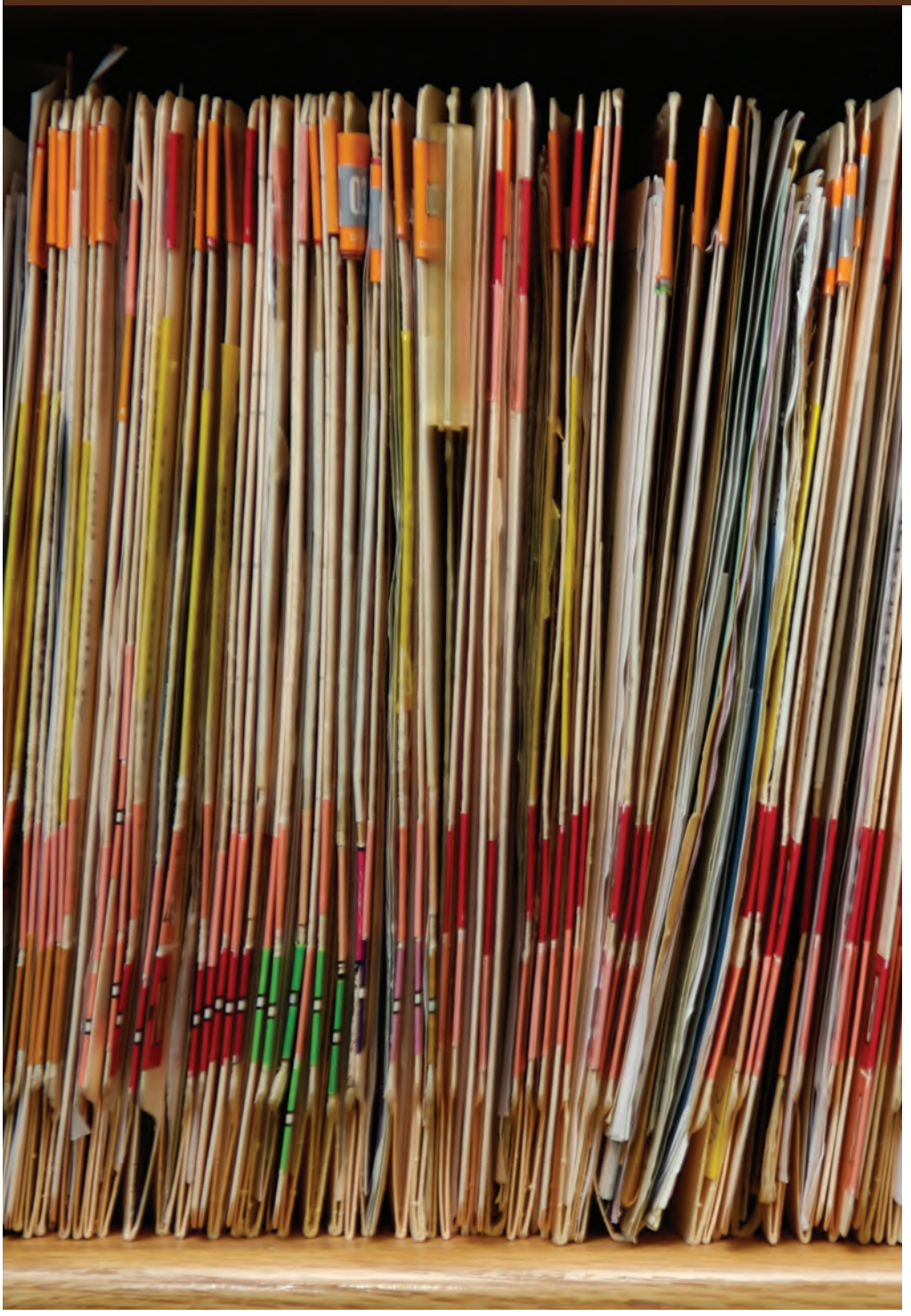
### In government

The Public Service Commission's *Information Technology Acceptable Usage Policy* (www.psc.gov.sk.ca) 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 appropriate lengths 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, etc.

Learn more in the following pages about records management, retention and disposal of records and information.

## 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 day to day activities. Schedules also determine how long each record should be kept. Schedules not only help you organize, retain and dispose of records in a safe and secure manner, they also promote greater accountability of information.

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

**In government**

*The Archives Act, 2004* 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 2006 (ARMS 2006):

- 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 Systems (ORS):

- A classification system and retention schedule for the operational records of an organization. Designed to be compatible with ARMS 2006.
- Unique to each organization and documents the mandated functions of your institution.
- Usually consists of client files, program files, and subject files.

Collectively, ARMS 2006 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 Saskatchewan Archives Board 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 Act, 2004*. 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, 2007)".
- Municipalities should consult approved retention schedules or contact the Ministry of Municipal Affairs 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!

Inappropriate disposal of records can result in privacy incidents (e.g. 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 Act, 2004*. The Saskatchewan Archives Board manages and administers the Records Disposition System which does the following:

1. Provides for a review to confirm that records are related to ARMS 2006 or to an appropriate ORS schedule and that the required retention periods have been met.
2. If the records are eligible for disposal, they are reviewed by an appraisal archivist.
3. Records of continuing historical value are acquired and preserved by the Saskatchewan Archives Board.
4. 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 Saskatchewan Archives Board 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 Office (ITO) will ensure the storage media on ITO-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, Ministry of Justice and Attorney General 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* on the Access and Privacy Branch website at: www.justice.gov.sk.ca/accessandprivacy

Additional information about privacy breach management can also be found at 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 about anything you have read in this handbook, 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. Local authorities may also have someone in this position.

  This is your first point of contact for access or privacy questions.

- 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.

**Refer to the outside back cover for information specific to your workplace.**

**For additional help**

- Access and Privacy Branch, Ministry of Justice and Attorney General
  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 reference tools to help manage access to information and privacy issues within public bodies in Saskatchewan including on-line training courses are available at: www.justice.gov.sk.ca/accessandprivacy

- Information Technology Office
  ITO provides information technology services for much of government. For more information go to: www.ito.gov.sk.ca

- Ministry of Advanced Education, Employment and Labour
  Universities, colleges and other post-secondary institutions in Saskatchewan can contact AEEL with specific questions about practices in this sector. For more information go to: www.aeel.gov.sk.ca

- Ministry of Education
  School divisions and libraries can contact Education with specific questions about practices in this sector at: www.education.gov.sk.ca or contact 787-6030.

- Ministry of Government Services
  Government 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. For more information go to: www.gs.gov.sk.ca

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

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

  E-mail: HIPAFOIhelp@health.gov.sk.ca

  Website: www.health.gov.sk.ca/health-information-protection-act

- Ministry of Municipal Affairs
  Municipal Affairs can provide advice on practices in the municipal sector. For more information go to: www.municipal.gov.sk.ca

- 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*.

  More information about the Commissioner and the role that office plays can be found at: www.oipc.sk.ca

- Queen's Printer
  The Office of the Queen's Printer publishes and distributes legislation, regulations and other government publications on behalf of the Government of Saskatchewan.

  Acts and regulations are available on the Queen's Printer web site at: www.qp.gov.sk.ca

- Saskatchewan Archives Board
  Records management, retention and disposal practices for government are managed by the Saskatchewan Archives Board. For more information please visit the Archives Board website at: www.saskarchives.com