

YOUR NAME: \_\_\_\_\_

DATE OF PRIVACY TRAINING: \_\_\_\_\_

---

---

# Privacy Rules!

---

---



Information Access  
and Privacy Protection

**2011**

Memorial University is entrusted with the personal information of its students, employees, alumni, donors, research participants, retirees and others and is committed to excellence in its management of this information.

---

---

# Privacy Tools!

---

---

This page left blank

## Table of Contents

Preamble .....	ii
Introduction to Privacy Concepts.....	1
Introduction to Privacy Legislation .....	3
Memorial University Privacy Policy.....	5
University Privacy Officer, IAPP Office, IAPP Advisory Committee and Unit Privacy Officers.....	6
Privacy Rules! .....	8
<b>Collection Rules</b> .....	<b>8</b>
<b>Use Rules</b> .....	<b>8</b>
<b>Disclosure Rules</b> .....	<b>9</b>
<b>Retention Rules</b> .....	<b>9</b>
<b>Security Rules</b> .....	<b>10</b>
<b>Accuracy Rules</b> .....	<b>10</b>
Privacy Tools! .....	11
<b>Collection Questionnaire</b> .....	<b>11</b>
<b>Privacy Notice</b> .....	<b>11</b>
<b>Privacy Compliance Checklist</b> .....	<b>12</b>
<b>Privacy Impact Assessment</b> .....	<b>13</b>
<b>Information Sharing Agreement</b> .....	<b>14</b>
<b>Contractor Privacy Schedule</b> .....	<b>14</b>
<b>Researcher Agreement</b> .....	<b>15</b>
<b>Confidentiality Agreements</b> .....	<b>15</b>
<b>Correction of Personal Information</b> .....	<b>16</b>
<b>Privacy Breach Protocol</b> .....	<b>16</b>
<b>Encryption</b> .....	<b>17</b>
<b>Email</b> .....	<b>17</b>
<b>Fax</b> .....	<b>18</b>
Other Stuff .....	19
<b>Social Insurance Numbers</b> .....	<b>19</b>
<b>Passwords</b> .....	<b>19</b>
<b>Disposal of Records</b> .....	<b>20</b>
Where to get more information .....	21

## Preamble

Memorial University's Privacy Policy requires that all employees take privacy training.

The *Privacy Rules! Privacy Tools!* training manual is developed by Memorial University's Information Access and Privacy Protection office and forms part of materials the office provides to participants in privacy training.

The IAPP Office offers scheduled two-hour sessions which are open to all members of the community. We also conduct training on request for specific groups. Full day privacy training seminars are offered to employees who are designated as unit privacy officers and those whose work is privacy-intensive.

The *Privacy Rules! Privacy Tools!* training manual will be updated from time to time.

Rosemary Thorne  
IAPP Coordinator  
Memorial University  
February 2011

# Introduction to Privacy Concepts

## What is Privacy?

Privacy encompasses:

- physical privacy
- freedom from surveillance
- privacy of one's surroundings
- privacy of one's person, and
- protection of personal information

It is a broad, all-encompassing concept that envelops a host of human concerns about various forms of intrusive behaviour, including wiretapping, surreptitious surveillance, and interception of mail, whether electronic or physical.<sup>1</sup>

This training is about information privacy.

## Definition of information privacy and why it is important

---

The Privacy Commissioner of Canada defines privacy as “ the right to control access to one's person and information about one's self. The right to privacy means that individuals get to decide what and how much information to give up, to whom it is given, and for what uses.”<sup>2</sup>

---

Information privacy is important because: first, our students, employees, alumni, donors, research participants, retirees and others rely on Memorial University's integrity, reputation and commitment to privacy protection in all aspects of its operations. Secondly, Memorial University as a public body is required to comply with the *Access to Information and Protection of Privacy Act* and other applicable legislation.

---

<sup>1</sup> Information Access and Protection of Privacy Certificate Program. (2008). *Information Access and Protection of Privacy Foundation*. Edmonton: University of Alberta.

<sup>2</sup> Privacy Commissioner of Canada: <http://www.priv.gc.ca/>

## What is Personal Information?

Protection of privacy legislation protects "personal information."

Personal information is "information about an identifiable individual." It includes a person's name, address, telephone number, age, health, financial and educational information, and identifying numbers and symbols like a student number and employee number. This is not an exhaustive list. Any information about an identifiable individual is that person's personal information. ( [Section 2](#) of [ATIPPA](#))

The University holds personal information belonging to students, faculty, staff, alumni, donors and others. Sometimes personal information may be regarded as sensitive personal information. Most often, people consider their health information to be sensitive personal information; others may feel that their personal financial information is particularly sensitive. In terms of privacy risks like unauthorized access, credit card numbers and social insurance numbers are considered to be sensitive personal information.

**Personal information** is defined in Section 2 of *ATIPPA*. It reads:

"personal information" means recorded information about an identifiable individual, including

- the individual's name, address or telephone number,
- the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,
- the individual's age, sex, sexual orientation, marital status or family status,
- an identifying number, symbol or other particular assigned to the individual,
- the individual's fingerprints, blood type or inheritable characteristics,
- information about the individual's health care status or history, including a physical or mental disability,
- information about the individual's educational, financial, criminal or employment status or history,
- the opinions of a person about the individual, and
- the individual's personal views or opinions

# Introduction to Privacy Legislation

## *Access to Information and Protection of Privacy Act (ATIPPA)*

The *Access to Information and Protection of Privacy Act (ATIPPA or the ATIPP Act)* is a Newfoundland and Labrador law which governs provincial public sector organizations – government departments, agencies, boards, commissions, municipalities, schools and school boards, and public post-secondary institutions. *Public body* is a defined term in *ATIPPA*.

*ATIPPA*:

- gives people a right of access to records
- gives people a right of access to personal information about themselves
- gives people a right to request correction of personal information about themselves if they believe it contains an error or omission
- prevents the unauthorized collection, use and disclosure of personal information by public institutions
- provides for an independent review of decisions made by public institutions under *ATIPPA*

*ATIPPA* protects **privacy** by placing limits on the collection, use and disclosure of personal information. As well, public institutions are required to ensure that personal information is held securely and is accessible only by those who are authorized under *ATIPPA*, for example, employees who need access to the information in order to carry out their job responsibilities.

## Other Privacy Legislation

### *Personal Information Protection and Electronic Documents Act (PIPEDA)*

The *Personal Information Protection and Electronic Documents Act* is a statute of Canada which applies to businesses and commercial activities.

The Privacy Commissioner of Canada has stated that *PIPEDA* generally does not apply to the core activities of universities.<sup>3</sup>

### *Privacy Act*

The *Privacy Act* of Newfoundland and Labrador establishes grounds for civil action in the event of unauthorized surveillance, recording, impersonation or use of personal communications or documents without the consent of the individual or a duly authorized representative.

### *Personal Health Information Act (PHIA)*

The *Personal Health Information Act* was passed by the Newfoundland and Labrador legislature in June 2008. *PHIA* recognizes the particular sensitivity of personal health information and addresses the challenges of privacy protection in the complex array of public and private entities involved in health care. *PHIA* is expected to be proclaimed in 2011.

---

<sup>3</sup> Privacy Commissioner of Canada. (nd). *Office of the Privacy Commissioner of Canada*. Retrieved March 31, 2009, from Fact Sheet: Municipalities, Universities, Schools and Hospitals: [http://privcom.gc.ca/fs-fi/02\\_05\\_d\\_25\\_e.asp](http://privcom.gc.ca/fs-fi/02_05_d_25_e.asp)

# Memorial University Privacy Policy

The Privacy Policy was adopted by the Board of Regents on September 11, 2008. This policy was developed to provide guidance to the University community and to respond to requirements of privacy legislation. It applies to all campuses and organizational units of Memorial University and all information in the custody and/or control of the University.

The Privacy Policy contains the following procedures:

- Procedure for administering privacy measures within a unit
- Procedure for challenging privacy compliance
- Procedure for checking privacy compliance
- Procedure for correcting/annotating personal information
- Procedure for giving researchers access to personal information
- Procedure for managing a privacy breach
- Procedure for retention of personal information

Procedures may be amended and added by approval of the IAPP Advisory Committee.

The Privacy Policy is available on the policy website at:

<http://www.mun.ca/policy/site/policy.php?id=145>

# University Privacy Officer, IAPP Office, IAPP Advisory Committee and Unit Privacy Officers

## University Privacy Officer

The university privacy officer is the position with overall management responsibility for privacy policy and procedures at the University. *This is a functional description, not a title.* The Information Access and Privacy Protection Coordinator is the university privacy officer.

## IAPP Office

The Information Access and Privacy Protection (IAPP) Office was created in November 2005 to assist the university in complying with the provincial *Access to Information and Protection of Privacy Act (ATIPPA)* and other applicable privacy legislation, as well as developing best practices in information access and privacy protection matters.

The IAPP Office manages formal information requests made under the *ATIPPA Act*.

As well, the IAPP Office is available to advise on access and privacy matters and to provide education and training to the university community.

## IAPP Advisory Committee

The IAPP Advisory Committee is a standing committee of the University, which has responsibility for advising the University Privacy Officer in the development and implementation of the University's privacy policy and procedures.

The IAPP Advisory Committee provides strategic direction and general guidance to the IAPP Office. They are responsible for recommending guidelines, policies, and procedures to ensure compliance with the *Access to Information and Protection of Privacy Act* and established best practices.

## Unit Privacy Officers

Each unit has a designated employee with responsibility for privacy. Unit Privacy Officers participate in a one-day privacy training seminar, focusing on how to use the Privacy Tools and assist other employees in their units.

# Employee Duties

Employees of the University are subject to the *ATIPP Act*.

All employees of Memorial University are responsible for the protection of the personal information to which they have access.

To protect personal information, employees should be familiar with the Privacy Policy and other policies concerning confidentiality and security.

University employees who act in good faith and who execute their employment responsibilities with a reasonable standard of care shall not be subject to discipline for privacy breaches.



# Privacy Rules!

Privacy rules were created to provide employees with some easy to use guidelines to protect privacy within their unit in accordance with the *ATIPP Act* and University policy. Be sure to take a look at the “**Privacy Rules! Privacy Tools!**” section of the IAPP website!

## Collection Rules

- Collect personal information only if you have authority under section 32
- Collect personal information directly from the individual concerned unless secondary collection is permitted, for example under sub-section 33(1)
- Add a Privacy Notice to all collections of personal information, which sets out the authority for the collection, the purpose for the collection and the contact details of an employee who can answer questions about the collection

**Reference: Section 32 and Section 33 of the *ATIPP Act***

---

## Use Rules



- Use personal information only for the purpose for which you collected it (stated on your Privacy Notice) or for a similar purpose
- Minimize your use of personal information
- Use for other limited purposes (consult the IAPP Office for advice)

**Reference: Section 38, Section 39 and Section 40 of the *ATIPP Act***

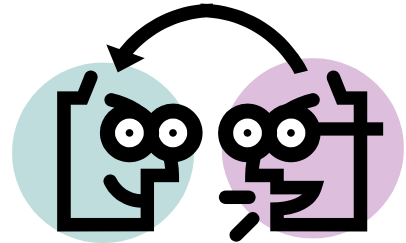
## Disclosure Rules

- Disclose if disclosure is required to fulfill the purpose of collection
- Disclose with consent of the individual(s) concerned
- Disclose for other limited purposes (consult the IAPP Office or General Counsel for advice)

**Reference: Section 39 of the ATIPPA Act**

Before you disclose information, consider the following:

- Are you permitted under *ATIPPA* to disclose this information?
- Can it be converted into unidentifiable data?
- Are you providing too much information? Keep the personal information disclosed at a minimum.



---

## Retention Rules

Different records have different retention schedules. They may hold *administrative, legal, financial, or archival value* to the University. It is important to check your **unit guidelines** for retention schedules, so that you don't dispose of records prematurely or keep records longer than is necessary.

Holding on to information longer than necessary can be as problematic as not retaining information long enough. Work together with your unit to ensure that you understand the Unit retention schedules, and the University's Records Management Policy.

- Units may have retention guidelines that require longer retention periods but personal information used to make a decision that directly affects an individual must be retained for a minimum of 12 months from its last use

**Reference: Section 37 of the ATIPPA Act**

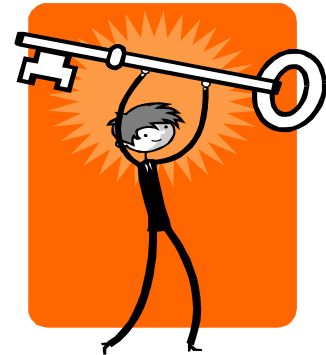
## Security Rules

Appropriate security measures should be used to secure the confidentiality, integrity and availability of personal information. The nature of such measures should be consistent with the sensitivity of the personal information involved. Access to personal information is to be restricted to duly authorized employees.

- Protect personal information against risks of unauthorized access, collection, use, disclosure and disposal regardless of the format in which it is held

The methods to protect personal information include:

- Physical controls (e.g., locked filing cabinets and restricted access to offices; after hours alarms and monitoring systems),
- Administrative controls (e.g., security clearances and other measures to limit access to personal information on a "need-to-know" basis as it relates to job duties), and
- Technological controls (e.g., the use of encryption, role-based user authorization and authentication, transaction logging, intrusion detection, etc.)



**Reference: Section 36 of the ATIPP Act**

---

## Accuracy Rules

- When you use personal information to make a decision affecting a person, make every effort to ensure that the information is accurate and complete.

*Remember:* under ATIPPA individuals have the right to request the correction of personal information, or an annotation to their file if no correction is made.

**Reference: Section 34 of the ATIPP Act**

# Privacy Tools!

Privacy tools are located on the IAPP website. These are valuable tools to help you become privacy compliant.

## Collection Questionnaire

Use a collection questionnaire to develop your privacy notice. It is used to assess the direct collection of personal information - from students, faculty, staff, alumni, donors or others – to ensure the collection is in compliance with *ATIPPA* and to help you identify all the purposes for which you are collecting the information.

Having all the uses identified at the time of collection is good practice. Using personal information for “secondary” purposes is not permitted under *ATIPPA*, so identifying all the uses up front will save you having to seek consent down the road for a secondary use.

The collection questionnaire is found at: <http://www.mun.ca/iapp/resources/Questionnaire2.pdf>

---

## Privacy Notice

Privacy Notices are **mandatory** when collecting personal information from individuals. A privacy notice can be easily added to existing forms and added to new forms being developed.

The law requires privacy notices to be added to all forms/documents/systems which collect personal information, including electronic collections. Privacy notices must state the authority and purpose for the collection and contact information of an employee who can answer questions about the collection.

Obtain written consent to a collection of sensitive personal information, including social insurance numbers, financial/banking information, health information and personal information which is collected for the purpose of disclosure outside the university and for information collected for an unusual purpose, for example, collecting students' opinions on non-curricular matters. As well, consent should be obtained when the intended use involves broad disclosure, e.g., publication of student information (on a website or in a written form).

A sample privacy notice:

All personal information collected by the \_\_\_\_\_ Program will be used solely for the administration and management of the program. Personal information is collected under the authority of the Memorial University Act (RSNL 1990 Chapter M-7) and is used for the purposes of program planning and human resource management. Questions about this collection and use of personal information may be directed to \_\_\_\_\_ at 709-864-XXXX.

See other samples of privacy notices at [www.mun.ca/iapp/resources/Sample\\_Notices2.pdf](http://www.mun.ca/iapp/resources/Sample_Notices2.pdf).

## Privacy Compliance Checklist

Completing a Compliance Checklist is **mandatory** under the University Privacy Policy for all new programs/projects involving personal information, except for research projects which receive appropriate ethics approval.



Use the Compliance Checklist to evaluate new projects involving the collection, use, retention and/or disclosure of personal information and identify privacy gaps and risks. The checklist is an Excel document:

Sheet 1 – How to use the checklist (one page overview of the Compliance Checklist)

Sheet 2 – Checklist – ATIPPA (checks compliance of your project/program with ATIPPA)

Sheet 3 – Checklist – CSA Code (checks compliance of your project/program with the Canadian Standards Association Model Code – PIPEDA; use if your project involves personal health information or is a commercial activity)

Sheet 4 – Approval page – approval of supervisor goes here

Sheet 5 – Scoring – Gives you a % score. RED indicates substantial risk of non-compliance; YELLOW indicates significant privacy risks; GREEN indicates good compliance posture (although some risks may be identified)

Sheet 6 – Warnings – contains warnings and suggestions about particular risk factors

Sheet 7 – Notes - notes about the checklist

The Compliance Checklist is found at: <http://www.mun.ca/iapp/resources/>

## Privacy Impact Assessment

A privacy impact assessment (PIA) may be advised for projects or initiatives that include:

- the collection of types or categories of personal information that have not previously been collected by Memorial University, or
- the use or disclosure of personal information in new ways, for new purposes, or for purposes that have not previously been disclosed to the subjects of the personal information.

The IAPP Coordinator reviews the results of privacy compliance checklists, and determines, along with the IAPP Advisory Committee, whether the project requires a full PIA assessment.

PIA's will include at a minimum the following information:

- The nature, objectives and purposes of the Project, initiative, software application, or Personal Information Bank that is the subject of the PIA, including its need for personal information.
- The types of personal information involved.
- The sources from which personal information is to be collected.
- The purposes for which personal information is to be used within the University.
- The recipients to whom personal information is to be disclosed.
- The legislative and policy authority for the collection, use and disclosure of personal information.
- The security measures to be applied for the protection of personal information from unauthorized use or disclosure.
- Plans for the periodic review or audit of personal information management practices, risks and outcomes.
- Details of any contractual arrangements involving the exchange of personal information other than basic business contact information.
- Potential privacy risks, planned measures to mitigate those risks, and the expected residual privacy risk that may remain after mitigation

More information on PIA's is available at: <http://www.mun.ca/policy/site/procedure.php?id=103>

## Information Sharing Agreement

An Information sharing agreement (ISA) may be used to detail and document the exact terms and conditions of disclosure to or collection from another public body in Newfoundland and Labrador. Of course, any collection or disclosure must be authorized under *ATIPPA*.

An ISA sets out just how the information will be transmitted, permitted uses, and other privacy considerations.

An Information Sharing agreement template is found at: <http://www.mun.ca/iapp/resources/>



---

## Contractor Privacy Schedule

A privacy schedule is **mandatory** under the University Privacy Policy for all agreements with consultants, contractors, and outside service providers.

A privacy schedule states the privacy obligations of the external party to Memorial University in respect of personal information. It ensures that the university remains in compliance with *ATIPPA* even though personal information may be disclosed to an outside service provider. The schedule includes sections on the purpose, collection, use, disclosure, retention, storage and access, inspection and non-compliance.

The privacy schedule should be appended as a schedule to the main contract/agreement or it may stand alone, with minimal amendments, if no other written contract/agreement is in place.

The Privacy Schedule is found at: <http://www.mun.ca/iapp/resources/>

## Researcher Agreement

The researcher agreement is **mandatory** under the University Privacy Policy.

The researcher agreement is required to be used whenever your unit is asked to disclose personal information to a researcher.

The Researcher Agreement is found at: [http://www.mun.ca/iapp/resources/Researcher\\_Agreement.pdf](http://www.mun.ca/iapp/resources/Researcher_Agreement.pdf)

---

## Confidentiality Agreements

All employees – whether student-employees, temporary and contractual employees or permanent employees – of the University are bound by University policy.

As a good privacy practice, have volunteers with access to confidential information in your unit sign a Confidentiality Agreement to ensure they uphold privacy law and policy requirements.

As well, a Confidentiality Agreement may be used for student-employees, and temporary or contractual employees. They should sign the agreement during their first week of employment.

Use the Confidentiality Agreement template available at [http://www.mun.ca/iapp/resources/ConfidentialityAgreement\\_0330.doc](http://www.mun.ca/iapp/resources/ConfidentialityAgreement_0330.doc)

What types of information are considered confidential?

- Financial
- Personal information
- Information relating to litigation
- etc.

## Correction of Personal Information

Under *ATIPPA*, people have a right to request correction of their records if they believe it contains an error or omission.

The obligation of the university to make a correction does not apply to opinions; it applies only to factual information. Requests for correction should be handled by the unit which has control of the record in question.

If corrections are made, third parties who have received this information in the preceding 12 months must be notified. Even if corrections are **not** made to the records, an annotation that the request was made and nothing was changed must be added to the records.

You can find on the IAPP website (<http://www.mun.ca/iapp/request/#b>) a form for the formal request for correction of personal information. This is treated as a last resort; whenever possible it is important to try to handle these situations informally.

---

## Privacy Breach Protocol

A privacy breach occurs if there is unauthorized access to or collection, use, disclosure or disposal of personal information. Such activity is "unauthorized" if it occurs in contravention of *ATIPPA* or, if applicable, a relevant provision of *PIPEDA*. An example of a privacy breach would be personal information becoming lost or stolen or personal information being mistakenly emailed to the wrong person.

The recommended privacy breach incident protocol has five steps. Step one is the responsibility of the individual or individuals who first become aware of the potential breach. The second through fifth steps are the responsibility of the University Privacy Officer, working in cooperation with other University officials and staff, as necessary.

Step 1: Reporting the Breach

Step 2: Containing the Breach

Step 3: Evaluating the Risks Associated with the Breach

Step 4: Notification

Step 5: Prevention

The Privacy Breach Protocol is set out in the Procedures forming part of the policy and may be found at <http://www.mun.ca/policy/site/procedure.php?id=106>.

## Encryption

Laptop computers and “flash” drives are a convenience to users who, from time to time, need to work from locations other than their offices. However, these convenience devices carry security risks.

Password-protect all portable computing devices such as laptops, PDAs, and Blackberries, and encrypt sensitive files stored on laptops and USB flash drives. Users who do not already have a preferred encryption solution are encouraged to avail of the encryption features built into Microsoft Office. Instructions on how to encrypt Word, Excel, and other Office documents can be found at:



<http://www.mun.ca/cc/services/security/resources/DocumentEncryption.php>

Please see the university’s Electronic Data Security Policy:

<http://www.mun.ca/policy/site/policy.php?id=188>

---

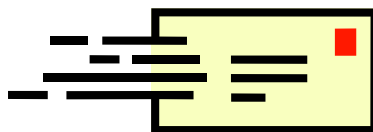
## Email

E-mails are subject to information and privacy legislation just as any other records in the custody and control of the University (with a few exceptions). For this reason, it is best that you avoid sending personal information in e-mails related to your job. However, if you do, you should take some precautions to make sure the information is not misused:

- Use non-identifiable terms rather than personal information, if possible
- Consider sending it as a password-protected Microsoft Office or Adobe Acrobat attachment. However, **don’t send the recipient the password by e-mail**; they should instead be exchanged in person or over the phone with the intended recipient
- Explicitly note if an e-mail message is confidential and not to be forwarded
- Add a confidentiality clause to your e-mail
- Before you e-mail personal information, confirm that you have the correct e-mail address

See the Guidelines for Using Personal Information in E-mail and Faxes located at:

[http://www.mun.ca/iapp/resources/Guidelines\\_for\\_Personal\\_Info\\_22Nov.pdf](http://www.mun.ca/iapp/resources/Guidelines_for_Personal_Info_22Nov.pdf)



## Fax

Just like e-mails, faxes are subject to information and privacy legislation. If you are dealing with personal information, it is better to use another form of communication. If the information is needed quickly and other methods, such as mail, are too slow you should make sure that you:

- Use non-identifiable terms rather than personal information, if possible
- Explicitly note if a message is confidential and not to be forwarded
- Add a confidentiality clause to all your faxes
- Always use a fax cover sheet, which clearly identifies the sender (with call-back particulars for the sender) and the intended recipient
- Before you fax personal information, confirm that you have the correct fax number
- Do not leave material you have faxed sitting on or near the fax machine. When you are faxing sensitive personal information, stay at the machine during faxing
- If you must fax sensitive personal information, consider phoning first to ensure that the intended recipient is the right person to receive the fax, the recipient will be there to receive it and to confirm the recipient's fax number. Ask the recipient to call to confirm receipt of the fax

### SAMPLE CONFIDENTIALITY NOTICE

This communication is intended for the use of the recipient to whom it is addressed, and may contain confidential, personal, and/or privileged information. Please contact us immediately if you are not the intended recipient of this communication, and do not copy, distribute, or take action relying on it. Any communication received in error should be deleted or destroyed.

More information is available on sending fax and email securely at  
[http://www.mun.ca/iapp/general/Guidelines\\_for\\_Personal\\_Info\\_22Nov.pdf](http://www.mun.ca/iapp/general/Guidelines_for_Personal_Info_22Nov.pdf)

## Other Stuff

### Social Insurance Numbers

SINs are required for income tax purposes and for certain financial transactions, like student loans. The SIN should not be used as a piece of identification and should not be recorded unless necessary to fulfill regulatory obligations which are part of the program you are operating.

For more information see: <http://www.mun.ca/iapp/general/SIN.pdf>

The SIN is an important piece of personal information; it can open the door to your personal information, it can be used in data matching, and it can be used in identity theft.

---

### Passwords

Keep your passwords confidential at all times.

New software to crack passwords is being created all of the time. For this reason it is important to create more difficult passwords. Make sure that your password is easy for you to remember, but not easy for others to guess. Stay away from birthdates and family names. When creating a password it is best to incorporate letters (case sensitive), numbers and symbols if possible. Also, to help protect yourself create “pass phrases.” Instead of using just one word, use a phrase. For example instead of “morning”, you could use “TopofThemorning2U!”

Passwords to avoid:

1. Passwords that can be associated with the account holder (i.e.. account numbers, names of family, pets, hobbies, birth dates, phone numbers, passwords derived from the above);
2. Words which appear in a dictionary;
3. Proper names;
4. Reversals of the above;
5. Passwords that may be more easily guessed if part of the password is known.

More information on passwords can be found in the Security of Confidential Information Housed in Administrative Systems Policy, located at:

[http://www.mun.ca/finance/policies\\_procedures/security\\_confidential\\_information.php#C-2.7](http://www.mun.ca/finance/policies_procedures/security_confidential_information.php#C-2.7)

## Disposal of Records

When disposing of records it is important to make sure unauthorized access to personal information does not occur. If the records are in a physical format such as paper or a CD they should be securely shredded.

If the item is unable to be shredded, then it should be destroyed manually.

When dealing with electronic records, the best method for destruction is repeated overwriting of the original data using specially designed software. Merely deleting the files or even reformatting the hard disk or USB drive will not suffice. Please refer to the procedures of the Data Removal Policy, located on the Memorial Policy website here, <http://www.mun.ca/policy/site/policy.php?id=159>. This policy is currently under review, and an updated version may be available in the near future.

For further information concerning available IT resources at Memorial contact Computing and Communications at:

<http://www.mun.ca/cc/services/servicedesk.php>

## Where to get more information

The Information Access and Privacy Protection Office is pleased to offer presentations and training on Information Access and Privacy Protection.

### IAPP Office

Memorial University of Newfoundland

[www.mun.ca/iapp](http://www.mun.ca/iapp)

208 Elizabeth Avenue

St. John's, NL

A1C 5S7

Telephone: 709-864-8753  
Fax: 709-864-2013  
Email: [rosemaryt@mun.ca](mailto:rosemaryt@mun.ca)

