Personal Information, Data Classification, Life Cycle and Best Practices

Table of Contents

Ten Principles for Working in a Privacy Protective Manner

The Canadian Standards Association (CSA) *Model Code for the Protection of Personal Information* (Q830) contains ten principles for working in a privacy protective manner.

1. **Accountability**
   An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

2. **Identifying Purposes**
   The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. **Consent**
   The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

4. **Limiting Collection**
   The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. **Limiting Use, Disclosure, and Retention**
   Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

6. **Accuracy**
   Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7. **Safeguards**
   Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. **Openness**
   An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9. **Individual Access**
   Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. **Challenging Compliance**
    An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Collection of Personal Information

Personal information is information about an identifiable individual or that identifies an individual, e.g. home or email address, student number, grades etc. Personal information does not include information about someone acting in a business or professional capacity, e.g. University employee name, position and work records are not usually personal information.

1. Collect personal information only if needed for established University functions.

2. Collect the minimum amount of personal information **needed** for the activity.

3. The University cannot legally collect personal information unless:
    a) Expressly authorized by statute (e.g. Huron University College Act), or
    b) Used for the purposes of law enforcement, or
    c) Necessary for the proper administration of a lawfully authorized activity.

4. Collect personal information directly from the person to whom it pertains, unless:
    a) The individual consents to collection from someone else, or
    b) To determine suitability for an honour or award, or
    c) To recognize outstanding achievement or distinguished service, or
    d) To conduct a proceeding or possible proceeding before a court or tribunal, or
    e) For law enforcement purposes.

5. Provide a Notice of Collection containing:
    a) The legal authority for the collection of the information,
    b) The principal purposes for which the information is intended to be used, and
    c) Title, address and phone number of a University official to address questions.

The University “collects” whenever it acquires, gathers or receives personal information.

Student personal information can be collected if needed for official activities such as registration, grading, granting degrees, discipline, program assessment, and where sharing of personal information is part of a program activity. Personal information can also be collected for purposes central to students’ University experience, like athletic activities.

For optional purposes, like recreational activities, student directories and clubs, student opt-in is usually necessary. In such cases, or if uncertain, clarify with Huron’s Privacy Officer.

Collecting personal information directly from an individual helps them to know and control how the University uses the information. Check with Huron’s Privacy Officer before collecting personal information from a source other than the individual.

The University uses a Notice of Collection to inform individuals of University purposes for personal information and to define allowable uses and disclosures by the University:

Huron University respects your privacy. Personal information that you provide to the University is collected pursuant to section 5 (Powers of Board) of the Huron University College Act, 2020. It is collected for the purpose of administering admissions, registration, academic programs, university-related student activities, activities of student societies, safety, financial assistance and awards, graduation and university advancement, and reporting to government agencies for statistical purposes. At all times it will be protected in accordance with the *Freedom of Information and Protection of Privacy Act*. If you have questions, please reach out to Huron's Privacy Officer at privacy@huron.uwo.ca or 519-438-7224 ext. 245.

For some activities, it may be necessary to add to or customize the above Notice.

Notices of Collection are generally given in writing on a form or website but can be given in any manner that ensures the individual has been notified.

For example, Notices can be spoken or read to an individual on the telephone or at a service desk or office. A precise "script" ensures consistency when notice is given verbally. You should create a written record that the Notice was read to and understood by the caller. Notices can also be prominently posted where collection occurs. A Notice can be printed on a form or on a sign notifying, for example, video security.

Use or Disclosure of Personal Information

1. Use and disclose personal information only for the purpose for which it was collected, for established University functions, or with consent of the individual.

2. Share personal information within the University only on a need-to-know basis. **Only** disclose personal information to a University employee, consultant or agent if they need the record in the performance of his/her duties and disclosure is necessary and proper in the discharge of the University's functions, e.g. don't respond to an email with Reply To All if only one individual has a need-to-know.

3. Even when there is a need-to-know, be cautious about emailing or faxing personal information and about leaving confidential information on a voice message.

4. Know which uses/disclosures of personal information **are** and are **not** permitted in your work.

5. To avoid inadvertent disclosure of personal information, do not include information about identifiable individuals unnecessarily in documents, emails, etc.

University practices provide for the use or disclosure of personal information only for established University purposes. Uses and disclosures of personal information should be:

1. Consistent with the purposes listed in University Notices of Collection.
2. Necessary to accomplish the (established University) purposes.
3. Consistent with faculty/program/divisional/University practices and activities.

When uncertain whether a use or disclosure of personal information is permitted, contact Huron's Privacy Officer.

Consent

Personal information may be used or disclosed with consent from the individual to whom the information pertains. Obtain written consent indicating:

- The particular personal information to be used/disclosed.
- The use being consented to or the entity to whom the information is to be disclosed.
- The date of the consent.

Where consent to use or disclose is obtained verbally, document it and ideally confirm through correspondence with the individual, indicating the above three points.

Where an individual purports to act as an agent for someone, the University has an obligation to verify whether or not the agent is properly authorized to obtain such information. Take special care where personal information is particularly sensitive, e.g. student grades. In such cases, contact the individual to whom the information relates to verify the status of his/her agent.

Purpose or Consistent Purpose

Personal information may be used or disclosed for the purpose(s) for which it was collected or for consistent purposes. A consistent purpose is one which: might reasonably have been expected at the time of collection; is "reasonably compatible" with the purpose for which the personal information was collected by the University; or consistent with the purpose(s) listed in the Notice of Collection. Contact Huron's Privacy Officer if uncertain. If a needed use or disclosure of personal information is not included in the Notice of Collection, contact Huron's Privacy Officer to discuss customization of the Notice.

Need-to-Know Disclosure -- For disclosures within the University

Personal information may be disclosed as necessary within the University on a need-to- know basis according to the "Need-to-Know Principle", which provides that:

Personal information may be provided to a University employee, agent or consultant, who needs the personal information for the performance of his/her duties, if the disclosure is necessary and proper in the discharge of the University's functions.

Personal information should be disclosed to agents or consultants only with a confidentiality agreement and/or having privacy protection built into the contract.

Responsibility for the need-to-know principle rests with the entire University. Both a University official seeking the personal information and an official who may disclose it are responsible for ensuring that the disclosure is proper. For example, an employee responsible for student data and a professor who requests the data are jointly responsible for following the need-to-know principle. The professor should only request personal information needed for the performance of duties, where the disclosure is necessary and proper for University functions. The employee must only release this specific personal information to a University official who is known to need it for proper purposes.

Need-to-know applies to required personal information in a document or record, but not necessarily to the entire document. Rather than sharing entire records or files, provide only the specific information needed by the individual making the request.

Law Enforcement Disclosure

Personal information may be disclosed to a law enforcement agency such as a police force, to aid a law enforcement investigation. However, the University may choose to require a warrant, summons or court order before such a disclosure. Except for emergency situations, always check law enforcement disclosures with Huron's Privacy Officer.

Compelling Circumstances Disclosure

The University should disclose personal information in compelling circumstances, where delay in sharing information could impact health or safety, e.g. disclosure of personal information to health care providers and/or family to help a distressed individual or to prevent a suicide. Try to consult with your manager or other appropriate University officials but you should act if you can't contact them. **Safety always takes precedence.**

Immediately contact emergency response services or police where there is apparent or imminent injury, threat, danger or violence.

Compassionate Circumstances Disclosure

The University may contact next-of-kin to inform them of injury, illness, or death. Personal information may be disclosed about the injured or deceased person to the relative or friend.

Uses and Disclosures to Avoid

Do not use or disclose personal information where it is merely convenient or desirable. For example, a software contractor need not see personal data, where depersonalized information could be used. Never compromise privacy for administrative convenience.

Avoid:

- Emailing or faxing personal information or leaving confidential information on a voicemail message.
- Sharing personal information with everyone in your workplace.
- Revealing personal information in a public setting while on your cell phone.

Retention of Personal Information

1. Know what personal information is contained in records with which you work.

2. Follow University retention schedules and requirements applicable to your records.

3. Retain personal information for at least one year after its last use.

All University offices should follow retention requirements for its records. Information of identifiable individuals must be retained for at least one year after the date of its last use. Record retention schedules are often longer to meet business, fiscal or legal requirements.

You need not retain personal information in the form that it was received, e.g. feel free to transcribe voicemail or print out and retain a hard copy of an e-mail.

For FIPPA access requests, retain all records until the matter is complete and all appeal periods have expired.

Do not destroy personal information less than one year after its last use unless you have the documented voluntary consent of the individual to whom it pertains.

Records Management

1. Establish and communicate which office/individual is responsible for creation, maintenance and disposal of records in your unit.

2. Only create records needed for business purposes or to demonstrate due diligence.

3. Record all necessary information, but nothing irrelevant or inappropriate.

4. Know who is authorized to access records with which you work.

5. Keep University records according to records retention schedules applicable to your operational area and discard insignificant transitory records on an on-going basis.

Records management practices should: align with and support business functions and requirements; support operational efficiency; be cost-effective; be simple for staff to implement; and apply to entire record life cycles from creation to disposal.

Because FIPPA defines "record" broadly, as "any record of information however recorded", all recorded information at the University falls under this practice. This includes hard copy, electronic, e-mail, audio/video records etc. on any recording or storage medium or system.

Records are needed for the University to: carry out its functions; achieve its goals; make informed decisions and demonstrate due diligence and accountability. It is important to quickly find records needed for business purposes.

Official records, such as decisions, practices, policies, legal papers, audits and public documents should meet the highest possible quality standards. You should also create quality professional records in your everyday work, including rough notes, drafts and routine matters. Although these "transitory" records are not intended to be permanent, while they exist, they are potentially releasable pursuant to legal obligations, such as access requests. Therefore, always create quality, professional records, including emails.

Only create records as needed to support work objectives. The following general parameters can help you to assess your documentation requirements.

1. Know which activities are your unit's and your position's responsibility.

2. Decide what to record; is it required by law or policy or operationally necessary?
3. Decide if a record is needed. Sometimes a telephone call can replace an email.
4. Do not record personal views, inappropriate comments or unnecessary information.

Identify and assign an office or individual to be responsible for each record category and type. That person/office will create, use, store or dispose of the record in question.

Follow records retention schedules to know how long and how to keep records, as well as their disposition, i.e. destroy or transfer to Off-Site Storage/Archives.

Data Classification Standard

All University data stored, processed, or transmitted on or through the University resources or where University business occurs can be classified as either **confidential, sensitive,** or **public,** and must be protected accordingly using appropriate measures consistent with the University's Data Handling Standard.

Confidential Data

Data is strictly protected by the provincial or federal regulations (FIPPA, PHIPA, PIPEDA), University policy, or contractual agreement and must be protected from unauthorized access, modification, distribution, and use. It should not reside on general purpose computers as it requires highest level of security controls and access management. If this data is compromised, it can cause significant or lasting impact to the reputation of an individual or University. This may include but not limited to

- Patient Medical/Health Information Record
- Student Records including grades and financial information
- Employee information
- Critical infrastructure details
- Any other Personally Identifiable Information (PII) as described in the above regulations

Sensitive Data

Data is protected by proprietary, ethical or privacy regulations and must be protected from unauthorized access, modification, distribution, and use. Data is available for use by members of the University community who have legitimate access to the data. If this data is compromised, it can cause a minor, short-term impact to the individual or University. This includes but not limited to

- Planning documents
- Internal internet websites
- Official meeting minutes before approval
- Employee / student email messages and network usage information
- Sensitive accounting information
- Internal project reports
- Department budget information

Information considered as sensitive could potentially become classified as confidential if when aggregated, can reveal personally identifiable information.

Public Data

Data is readily available to any member of the University community or general public. There is no legal restriction to access and use. It may include personal information collected with consent from individuals. Little or no impact to the reputation of individual or University, if data is compromised. This includes but not limited to

- Any data that has been publicly published through official channels such as press release, newsletter, maps, faculty and staff directory, financial statements.
- Any information that does not comply with confidential or sensitive classification standard.

Data Handling Standard

Understanding

The data management cycle begins with the understanding of what data is, how it has been classified and where it will be located. This cycle is iterative and will keep looping back to understanding the data. For example, data may need to be re-classified as it changes and becomes aggregated. Data can be classified into three categories based on the Data Classification Standard.

Creating

There should be a specified purpose for creating data. Data can be created afresh i.e. new data source or from existing data sources. It is important to ensure that only the necessary data is created, collected and stored.

Storing

Once data is classified appropriately, it is pertinent to know how and where different data can be stored to safeguard it from unauthorized access and use. Data can be in either paper or electronic format with each one having its own security and access control in place.

CONFIDENTIAL DATA

PAPER

- File cabinets housing confidential data must always be locked.
- Data must not be kept or placed where an unauthorized individual can access it.

ELECTRONIC

- Data must not be stored on personal devices. It can be saved on a dedicated central computer system or Western University's OneDrive.
- Additional security measures listed below must be put in place to safeguard the computer system storing the confidential data.
    - Hardening of the Operating System.
    - Data stored must be encrypted.
    - Two-factor authentication (2FA) is required for the computer system storing the data.
    - Access to the system must be restricted.
    - Access logs to the computer system must be maintained.
    - Data must not be stored on portable storage drives.

SENSITIVE DATA

PAPER

- File cabinets housing sensitive data must always be locked.
- Data should not be kept or placed where an unauthorized individual can access it.

ELECTRONIC

- Data can be stored on personal devices.
- Strong password and two-factor authentication (2FA) is recommended on the devices.
- Data stored may be encrypted or password-protected.
- Data can be stored on Western University's OneDrive and portable storage drives.
- Portable storage drives should be stored in file cabinets which must always be locked.

PUBLIC DATA

- No restriction on where data can be stored.

Using

This deals with how the different classes of Western data can be used appropriately. Data either in paper or electronic format should only be used for the specified purpose.

CONFIDENTIAL DATA

PAPER

- Access to file cabinets must be handled by trained and authorized staff.
- Access records must be maintained.
- Whenever the data is in use, it must not be left unsupervised.

ELECTRONIC

- Read/write access must be reviewed and audited regularly, as well as revoked when no longer needed.
- When in use, care must be taken to avoid unnecessary exposure.

SENSITIVE DATA

PAPER

- Access to file cabinets should be handled by trained staff.
- Data should not be left unsupervised.

ELECTRONIC

- Data should not be placed where unauthorized users can access it.
- Auditing and access control must be in place.

PUBLIC DATA

- No restriction on how data is used.

Sharing

It is pertinent to know how the different classes of University data can be shared and the processes involved. Whenever data is shared, it is recommended to use a data sharing agreement that defines the following details:

- how the data will be used

- the duration of usage/sharing
- what happens when the data is no longer in use
- any restrictions on usage
- how the data will be secured

CONFIDENTIAL DATA

PAPER

- If data is to be sent by post, registered mail must be used for the purpose.
- The internal/inner envelope must have “confidential” written on it while the external/outer envelope should only carry the address.
- Access to the file cabinet must be restricted.
- Access records to the file cabinet must be maintained.

ELECTRONIC

- Data must be transmitted using an encrypted communication channel (HTTPS).
- Data may be encrypted, or password protected when sent through e-mail.
- Data must not be sent with external e-mail accounts such as yahoo, gmail, etc.
- Access to the data must be restricted.
- Data should be shared based on a need-to-know basis.
- The use of data sharing agreement is recommended.

SENSITIVE DATA

PAPER

- If data is being sent by post, the internal/inner envelope should have “sensitive” written on it while the external/outer envelope should only carry the address.
- Access to the file cabinet should be restricted.
- Access records should be maintained.

ELECTRONIC

- Data must be transmitted using an encrypted communication channel.
- If data must be sent through e-mail, it may be encrypted or password-protected.
- Data should not be sent with external e-mail accounts such as yahoo, gmail, etc.
- Access logs to the data/drive where data is stored should be maintained.
- Data sharing agreement may be used where warranted.

PUBLIC DATA

- No restriction on how data is used.

Archiving

As part of the Records Retention and Disposal Schedule, records may need to be archived and stored off-site.

How do I archive my records/files?

Destruction

Portable storage devices

Apply the same procedures used for the disposal of paper records.

- Shredders: There are many types of shredders on the market that can be used to dispose of CDs, magnetic tape, etc.

Removing data from hard drives

- Workstations: use DBAN (http://dban.sourceforge.net/) to fully 'sanitize' the hard drive. Options include:
- Self service: download the software from Sourceforge (http://dban.sourceforge.net/) and follow the instructions provided.

Hard Drive Destruction Service

- When data cannot be fully removed from a hard drive, the hard drive MUST be removed from the workstation or server and physically destroyed.

If any assistance is required destroying digital storage devices, contact Huron Information Technology Services (ITS) by submitting a Jira request.

Individual Best Practices

Every individual has a personal responsibility to ensure they access data in a secure and private manner. Users must be familiar with the classification of data they work with and employ appropriate measures to respect data integrity and confidentiality. Below is a list of best practices and recommendations that an individual can and should employ. It is also recommended to annually complete Cybersecurity Awareness Training so that you are educated to detect social engineering attacks and recognize cyber threats, and other emerging vectors impacting privacy.

Accounts & Passwords

- Use complex passwords with a mix of upper and lowercase letters, numbers, and special characters. It is recommended that passwords are longer than 10 characters.
- Never write down a password or save a password where others can access it.
- Do not use the same password for all your accounts.
- Use Multi-Factor Authentication or Two Factor Authentication wherever possible.
- Use passcodes or other authentication mechanisms on mobile devices where sensitive information is available.
- If passwords must be shared, only share them in a secure manner. Do not send an email with a username and password within it. It is better practice to share the password over the phone, but ensure unauthorized users are not listening in.
- Make a point to update your password routinely.
- Use a password manager to confidentially store multiple passwords.

Software

- Always install software and operating system updates when they become available.
- Partner with IT to install software - be mindful of the software and applications that you use. When downloading and installing new software, ask yourself: is this software secure, does it come from a trusted source?
- Use Antivirus and scan your devices routinely. If you suspect you may have a virus, report it to Huron ITS.

Privacy in Social Settings

- Use privacy screens if your computer is in a public location or an area with high foot-traffic.
- Lock your computer to the login screen when you leave your desk.
- Be aware of the conversations you have. Ensure that no one is eavesdropping.
- Be overly cautious when sharing organizational and personal information.
- Know that imposters exist and that they may try to leverage information or impersonate a colleague or superior.
- Be aware of phishing attempts and scams and know how to recognize these attacks.
- Do not open emails or click on links from people that you do not know.

Data Handling

- Always back up your data to a secure location. Secure locations include network and authorized cloud storage providers.
- MANDATORY: Do not save confidential or critical data on your local systems.
- Dispose of data in a secure manner. Ask IT Services for assistance if you are unsure.
- Do not use USB flash drives, or other removable media.

Physical Privacy

- Lock your office door, desk drawers and storage cabinets. Do not leave keys in accessible locations.
- Do not leave personal information in a vehicle.
- Keep a clean desk. Do not leave confidential or sensitive information out in the open.
- Shred old documents when they are no longer needed.
- Don’t print private documents and take them home.
- Use the Private Print feature when printing confidential or sensitive information.
- Don’t print using publicly available, off-campus printers.
- Follow the organization’s document retention policy for both physical and electronic information.

Networks

- Do not access confidential or sensitive information over public networks, or publicly available computers (Starbucks WiFi, Public Libraries, etc.).
- Use a VPN if you are connected from a location that is not your workplace or home.
- Ensure the firewall is always enabled on your devices.

Incident Response

If you suspect an incident has occurred, disconnect your device from any networks and immediately report the incident to your superior and Huron ITS. If you believe an account has become compromised, change the password immediately.

References

Western University
Cyber Smart: Policies, Compliance & Risk Management

For any questions or concerns, please reach out to Huron's Privacy Officer:
privacy@huron.uwo.ca.