APPENDIX “A”

PRINCIPLES SET OUT IN THE NATIONAL STANDARD OF CANADA ENTITLED
MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION
CAN/CSA-Q830-96

1. Be accountable

Your responsibilities

- Comply with all 10 of the principles
- Appoint an individual (or individuals) to be responsible for your organization's compliance.
- Protect all personal information held by your organization or transferred to a third party for processing.
- Develop and implement personal information policies and practices.

How to fulfil these responsibilities

- Give your designated privacy official senior management support and the authority to intervene on privacy issues relating to any of your organization's operations.
- Communicate the name or title of this individual internally and externally (e.g. on Web sites and in publications).
- Analyze all personal information handling practices including ongoing activities and new initiatives, using the following checklist to ensure that they meet fair information practices:
    - What personal information do we collect?
    - Why do we collect it?
    - How do we collect it?
    - What do we use it for?
    - Where do we keep it?
    - How is it secured?
    - Who has access to or uses it?
    - To whom is it disclosed?
    - When is it disposed of?
- Develop and implement policies and procedures to protect personal information:
    - define the purposes of its collection
    - obtain consent
    - limit its collection, use and disclosure
    - ensure information is correct, complete and current
    - ensure adequate security measures

- develop or update a retention and destruction timetable
- process access requests
- respond to inquiries and complaints

- Include a privacy protection clause in contracts to guarantee that the third party provides the same level of protection as your organization does.
- Inform and train staff on privacy policies and procedures.
- Make information available explaining these policies and procedures to customers (e.g. in brochures and on Web sites).

TIPS

Train your front-line and management staff and keep them informed, so they can answer the following questions:

- How do I respond to public inquiries regarding our organization's privacy policies?
- What is consent? When and how is it to be obtained?
- How do I recognize and process requests for access to personal information?
- To whom should I refer complaints about privacy matters?
- What are the ongoing activities and new initiatives relating to the protection of personal information at our organization?

When transferring personal information to third parties, ensure that they:

- Name a person to handle all privacy aspects of the contract.
- Limit use of the personal information to the purposes specified to fulfil the contract.
- Limit disclosure of the information to what is authorized by your organization or required by law.
- Refer any people looking for access to their personal information to your organization.
- Return or dispose of the transferred information upon completion of the contract.
- Use appropriate security measures to protect the personal information.
- Allow your organization to audit the third party's compliance with the contract as necessary.

2. Identify the purpose

Your organization must identify the reasons for collecting personal information before or at the time of collection.

Your responsibilities

- Before or when any personal information is collected, identify why it is needed and how it will be used.
- Document why the information is collected.

- Inform the individual from whom the information is collected why it is needed.
- Identify any new purpose for the information and obtain the individual's consent before using it.

How to fulfil these responsibilities

- Review your personal information holdings to ensure they are all required for a specific purpose.
- Notify the individual, either orally or in writing, of these purposes.
- Record all identified purposes and obtained consents for easy reference in case an individual requests an account of such information.
- Ensure that these purposes are limited to what a reasonable person would expect under the circumstances.

TIPS

- Define your purposes for collecting data as clearly and narrowly as possible so the individual can understand how the information will be used or disclosed.
- Avoid overly broad purposes as they may conflict with the knowledge and consent principle.
- Examples of purposes include:
    - opening an account
    - providing benefits to employees
    - sending out association membership information
    - identifying customer preferences

3. Obtain consent

Your responsibilities

- Inform the individual in a meaningful way of the purposes for the collection, use or disclosure of personal data.
- Obtain the individual's consent before or at the time of collection, as well as when a new use is identified.

How to fulfil these responsibilities*

- Obtain consent from the individual whose personal information is collected, used or disclosed.
- Communicate in a manner that is clear and can be reasonably understood.
- Record the consent received (e.g. note to file, copy of e-mail, copy of check-off box).
- Never obtain consent by deceptive means.
- Do not make consent a condition for supplying a product or a service, unless the information requested is required to fulfil an explicitly specified and legitimate purpose.

- Explain to individuals the implications of withdrawing their consent.
- Ensure that employees collecting personal information are able to answer an individual's questions about the purposes of the collection.

TIPS

- Consent is normally obtained from the individual whose personal information is collected, used or disclosed.
- For an individual who is a minor, seriously ill, or mentally incapacitated, consent may be obtained from a legal guardian, or person having power of attorney.
- Consent is only meaningful if the individuals understand how their information will be used.
- Consent clauses should:
    - be easy to find
    - use clear and straightforward language
    - not use blanket categories for purposes, uses and disclosures
    - be specific as possible about which organizations handle the information.
- Consent can be obtained in person, by phone, by mail, via the Internet etc.
- The form of consent should take into consideration:
    - reasonable expectations of the individual
    - circumstances surrounding the collection
    - sensitivity of the information involved.
- Express consent should be used whenever possible and in all cases when the personal information is considered sensitive. Relying on express consent protects both the individual and the organization.

4. Limit collection

Your responsibilities

- Do not collect personal information indiscriminately.
- Do not deceive or mislead individuals about the reasons for collecting personal information.

How to fulfil these responsibilities

- Limit the amount and type of the information gathered to what is necessary for the identified purposes.
- Identify the kind of personal information you collect in your information-handling policies and practices.
- Ensure that staff members can explain why the information is needed.

TIPS

- By reducing the amount of information gathered, you can lower the cost of collecting, storing, retaining and ultimately archiving data.
- Collecting less information also reduces the risk of inappropriate uses and disclosures.

5. Limit use, disclosure and retention

Your responsibilities

- Use or disclose personal information only for the purpose for which it was collected, unless the individual consents, or the use or disclosure is authorized by the Act.
- Keep personal information only as long as necessary to satisfy the purposes.
- Put guidelines and procedures in place for retaining and destroying personal information.
- Keep personal information used to make a decision about a person for a reasonable time period. This should allow the person to obtain the information after the decision and pursue redress.
- Destroy, erase or render anonymous information that is no longer required for an identified purpose or a legal requirement.

How to fulfil these responsibilities

- Document any new purpose for the use of personal information.
- Institute maximum and minimum retention periods that take into account any legal requirements or restrictions and redress mechanisms.
- Dispose of information that does not have a specific purpose or that no longer fulfils its intended purpose.
- Dispose of personal information in a way that prevents improper access. Shredding paper files or deleting electronic records are ideal.
- Establish policies setting out the types of information that need to be updated. An organization can reasonably expect an individual to provide updated information in certain circumstances (e.g. change of address for a magazine subscription).

TIPS

- It may be less onerous and complicated to destroy or erase information than to make personal information anonymous.
- Conduct regular reviews to help determine whether information is still required. Establish a retention schedule to make this easier.

6. Be accurate

Your responsibilities

- Minimize the possibility of using incorrect information when making a decision about the individual or when disclosing information to third parties.

How to fulfil these responsibilities

- Keep personal information as accurate, complete and up to date as necessary, taking into account its use and the interests of the individual.
- Update personal information only when necessary to fulfil the specified purposes.
- Keep frequently used information accurate and up to date unless there are clearly set out limits to this requirement.

TIPS

- One way to determine if information needs to be updated is to ask whether the use or disclosure of out of date or incomplete information would harm the individual.
- Apply the following checklist for accuracy:
    - List specific items of personal information required to provide a service.
    - List the location where all related personal information can be retrieved.
    - Record the date when the personal information was obtained or updated.
    - Record the steps taken to verify accuracy, completeness and timeliness of the information. This may require reviewing your records or communicating with the client.

7. Use appropriate safeguards

Your responsibilities

- Protect personal information against loss or theft.
- Safeguard the information from unauthorized access, disclosure, copying, use or modification.
- Protect personal information regardless of the format in which it is held.

How to fulfil these responsibilities

- Develop and implement a security policy to protect personal information.
- Use appropriate security safeguards to provide necessary protection:
    - physical measures (locked filing cabinets, restricting access to offices, alarm systems)
    - technological tools (passwords, encryption, firewalls)
    - organizational controls (security clearances, limiting access on a "need-to-know" basis, staff training, agreements).
- Make your employees aware of the importance of maintaining the security and confidentiality of personal information.
- Ensure staff awareness by holding regular staff training on security safeguards.
- The following factors should be considered in selecting appropriate safeguards:
    - sensitivity of the information

- amount of information
- extent of distribution
- format of the information (electronic, paper, etc.)
- type of storage.

- Review and update security measures regularly.

TIPS

- Make sure personal information that has no relevance to the transaction is either removed or blocked out when providing copies of information to others.
- Keep sensitive information files in a secure area or computer system and limit access to individuals on a "need-to-know" basis only.

8. Be open

Your responsibilities

- Inform customers, clients and employees that you have policies and practices for the management of personal information.
- Make these policies and practices understandable and easily available.

How to fulfil these responsibilities

- Ensure front-line staff is familiar with the procedures for responding to individual inquiries.
- Make the following available:
  - name or title and address of the person who is accountable for your organization's privacy policies and practices
  - name or title and address of the person to whom access requests should be sent
  - how an individual can gain access to his or her personal information
  - how an individual can complain to your organization
  - brochures or other information that explain your organization's policies, standards or codes
  - a description of what personal information is made available to other organizations (including subsidiaries) and why it is disclosed.

TIPS

- Information about these policies and practices should be made available in person, in writing, by telephone, in publications or on your organization's Web site. The information presented should be consistent, regardless of the format.

9. Give individuals access

Your responsibilities

- When requested, inform individuals if you have any personal information about them.
- Explain how it is or has been used and provide a list of any organizations to which it has been disclosed.
- Give individuals access to their information.
- Correct or amend any personal information if its accuracy and completeness is challenged and found to be deficient.
- Provide a copy of the information requested, or reasons for not providing access, subject to exceptions set out in Section 9 of the Act (see page 18).
- An organization should note any disagreement on the file and advise third parties where appropriate.

How to fulfil these responsibilities

- Provide any help the individual needs to prepare a request for access to personal information.
- Your organization may ask the individual to supply enough information to enable you to account for the existence, use and disclosure of personal information.
- Respond to the request as quickly as possible and no later than 30 days after receipt of the request.
- The normal 30-day response time limit may be extended for a maximum of 30 additional days, according to specific criteria set out at Subsection 8(4) of the Act:
    - if responding to the request within the original 30 days would unreasonably interfere with activities of your organization
    - if additional time is necessary to conduct consultations
    - if additional time is necessary to convert personal information to an alternate format.
- If your organization extends the time, you must notify the individual making the request within 30 days of receiving the request, and of his or her right to complain to the Privacy Commissioner of Canada.
- Give access at minimal or no cost to the individual.
- Notify the individual of the approximate costs before processing the request and confirm that the individual still wants to proceed with the request.
- Give individuals access to their personal information.
- Make sure the requested information is understandable. Explain acronyms, abbreviations and codes.
- Send any information that has been amended, where appropriate, to any third parties that have access to the information.
- Inform the individual in writing when refusing to give access, setting out the reasons and any recourse available.
- There are some exceptions to the principle of providing access (see page 18 of this guide).

TIPS

- Keep a record of where the information can be found to make retrieval easier.
- Never disclose personal information unless you are sure of the identity of the requestor and that person's right of access.
- Record the date of receipt of the request for the information.
- Ensure that staff know how to identify an access request and to whom it should be referred within the organization.

10. Provide recourse

Your responsibilities

- Develop simple and easily accessible complaint procedures.
- Inform complainants of their avenues of recourse. These include your organization's own complaint procedures, those of industry associations, regulatory bodies and the Office of the Privacy Commissioner of Canada.
- Investigate all complaints received.
- Take appropriate measures to correct information handling practices and policies.

How to fulfil these responsibilities

- Record the date a complaint is received and the nature of the complaint (e.g. delays in responding to a request, incomplete or inaccurate responses, or improper collection, use, disclosure or retention).
- Acknowledge receipt of the complaint promptly.
- Contact the individual to clarify the complaint, if necessary.
- Assign the matter to a person with the skills necessary to review it fairly and impartially and provide that individual with access to all relevant records, employees or others who handled the personal information or access request.
- Notify individuals of the outcome of investigations clearly and promptly, informing them of any relevant steps taken.
- Correct any inaccurate personal information or modify policies and procedures based on the outcome of complaint, and ensure that staff in the organization are aware of any changes to these policies and procedures.

TIPS

- Ensure that staff is aware of policies and procedures for complaints, and to whom these complaints should be referred within the organization.
- Record all decisions to ensure consistency in applying the Act.
- Handling a complaint fairly and appropriately may help to preserve or restore the individual's confidence in your organization.