

SCHEDULE 1

(Section 5)

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

**4.1 Principle 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.

**4.1.1**

Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

**4.1.2**

The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.

**4.1.3**

An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

**4.1.4**

Organizations shall implement policies and practices to give effect to the principles, including

- (a) implementing procedures to protect personal information;
- (b) establishing procedures to receive and respond to complaints and inquiries;
- (c) training staff and communicating to staff information about the organization's policies and practices; and
- (d) developing information to explain the organization's policies and procedures.

## **4.2 Principle 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.

### **4.2.1**

The organization shall document the purposes for which personal information is collected in order to comply with the Openness principle (Clause 4.8) and the Individual Access principle (Clause 4.9).

### **4.2.2**

Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfil these purposes. The Limiting Collection principle (Clause 4.4) requires an organization to collect only that information necessary for the purposes that have been identified.

### **4.2.3**

The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

### **4.2.4**

When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to the Consent principle (Clause 4.3).

### **4.2.5**

Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

### **4.2.6**

This principle is linked closely to the Limiting Collection principle (Clause 4.4) and the Limiting Use, Disclosure, and Retention principle (Clause 4.5).

## **4.3 Principle 3 — Consent**

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

Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for

the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.

#### **4.3.1**

Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

#### **4.3.2**

The principle requires “knowledge and consent”. Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

#### **4.3.3**

An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.

#### **4.3.4**

The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

#### **4.3.5**

In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual’s name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual’s request constitutes consent for specific

purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

#### **4.3.6**

The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

#### **4.3.7**

Individuals can give consent in many ways. For example:

(a) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;

(b) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;

(c) consent may be given orally when information is collected over the telephone; or

(d) consent may be given at the time that individuals use a product or service.

#### **4.3.8**

An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.

### **4.4 Principle 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.

#### **4.4.1**

Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Clause 4.8).

#### **4.4.2**

The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

#### **4.4.3**

This principle is linked closely to the Identifying Purposes principle (Clause 4.2) and the Consent principle (Clause 4.3).

### **4.5 Principle 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 fulfilment of those purposes.

#### **4.5.1**

Organizations using personal information for a new purpose shall document this purpose (see Clause 4.2.1).

#### **4.5.2**

Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.

#### **4.5.3**

Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

#### **4.5.4**

This principle is closely linked to the Consent principle (Clause 4.3), the Identifying Purposes principle (Clause 4.2), and the Individual Access principle (Clause 4.9).

### **4.6 Principle 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.

#### **4.6.1**

The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

#### **4.6.2**

An organization shall not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected.

#### **4.6.3**

Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

### **4.7 Principle 7 — Safeguards**

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

#### **4.7.1**

The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

#### **4.7.2**

The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.

#### **4.7.3**

The methods of protection should include

- (a) physical measures, for example, locked filing cabinets and restricted access to offices;
- (b) organizational measures, for example, security clearances and limiting access on a “need-to-know” basis; and
- (c) technological measures, for example, the use of passwords and encryption.

#### **4.7.4**

Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

#### **4.7.5**

Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).

### **4.8 Principle 8 — Openness**

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

#### **4.8.1**

Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

#### **4.8.2**

The information made available shall include

- (a) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;
- (b) the means of gaining access to personal information held by the organization;
- (c) a description of the type of personal information held by the organization, including a general account of its use;
- (d) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and
- (e) what personal information is made available to related organizations (e.g., subsidiaries).

#### **4.8.3**

An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.

#### **4.9 Principle 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.

Note: In certain situations, an organization may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

##### **4.9.1**

Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

##### **4.9.2**

An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.

##### **4.9.3**

In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual.

##### **4.9.4**

An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.

##### **4.9.5**

When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the

nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

#### **4.9.6**

When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.

### **4.10 Principle 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.

#### **4.10.1**

The individual accountable for an organization's compliance is discussed in Clause 4.1.1.

#### **4.10.2**

Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.

#### **4.10.3**

Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist. For example, some regulatory bodies accept complaints about the personal-information handling practices of the companies they regulate.

#### **4.10.4**

An organization shall investigate all complaints. If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.