Appendix 1

Personal Information Protection Act (PIPA)

Best Practices for Protecting Personal Information

Although most nonprofit/voluntary sector organizations are not required by law to adhere to the Personal Information Protection Act (2004), it is an effective benchmark to use in creating information protection policy for any organization that collects personal information about their clients.

The following are suggestions for collecting and storing personal information responsibly and safely. If you have any questions or are interested in learning more, please email scip@volunteeralberta.ab.ca re: PIPA Best Practices.

- **Reasonable Purpose**
  Under PIPA, organizations may only collect, use and disclose personal information for purposes that are reasonable. In simpler terms, you need a *good reason* to collect the information.

  Generally, a reasonable purpose or good reason would be related to a service or activity of your organization. For example, if you run a community sports league, certain personal information is necessary to register a child and provide the sports program.

- **Storing Information**
  Under PIPA, your organization can keep personal information for as long as you need it for legal or business purposes.

  Personal information that you no longer need (e.g. contact information about former clients or staff) must be securely destroyed after a reasonable amount of time – one year is a good guideline but you might have legal reasons for keeping certain information (such as financial or tax records) for a longer time.

- **Privacy Contact**
  Under PIPA, when your organization collects personal information from an individual you must provide a contact person to whom questions can be directed about the collection.

  This "privacy contact" person can be a paid staff member, volunteer or board member. The contact person needs to have a basic understanding of the organization's privacy practices in order to respond to questions from the public appropriately.

- **Consent**
  Organizations subject to PIPA need consent to collect, use and disclose personal information about clients.

  When you obtain consent under PIPA, you must *notify* your clients of the information you collect, and how you use it. This *notice* can be included on a membership application or registration form, or may be given orally.

  Express Consent
  Obtaining *express consent* is the best practice. You may obtain express consent in writing or orally. If the information is sensitive it is a good idea to get consent in writing or to make a note that you asked for and received oral consent. Sensitive information is information such as Social Insurance Numbers, medical information, financial information, reference checks, and date of birth together with name and address.

  Sometimes you collect information for one purpose and may want to use it for another reason later on. For example, a sports league collects a child's contact information at the time of registration; the league might want to use that information to promote other programs. The league will need to obtain consent for that second purpose.

  If you disclose the personal information outside of your organization, you need consent to do so. For example, becoming a member in the local chapter of a society often means *also* becoming a member of the provincial or national society. If a local chapter discloses a member's information to a provincial or national chapter for membership purposes, the local chapter must inform the member and obtain consent.

  You can often obtain consent for all these different purposes at the same time – when you initially collect the information.

Implied Consent

In some situations, it is obvious what information is being collected and why. For example, if a client hands you a credit card to pay for her membership fee, you do not need to tell her that you are collecting her credit card information to process the payment! In this situation, there is *implied consent* to use the credit card information. When can you rely on implied consent?

You *may* use implied consent if:

- A client voluntarily gives you information, and
- The reason you need the information is obvious, and
- It is reasonable in that situation to volunteer the information

- **Employee/Volunteer Information**

  Your organization does not have to obtain consent from employees or volunteers to collect, use or disclose their personal employee information. Giving notice is enough if the information is related to establishing, managing, or terminating the employment or volunteer relationship. Notice should be given before the information is collected. Giving notice means telling your employees and volunteers what information you collect, use or disclose and why.

  Under PIPA, you can collect, use or disclose that information without consent, with two conditions:

  - The purpose is related to the employees' or volunteers' work (consent is required for other purposes); *and*
  - You tell (provide notice to) your employees or volunteers about the collection, use or disclosure, along with the purposes.

- **Protecting Information**

  Under PIPA, your organization is responsible for protecting the personal information you have about staff and clients by using reasonable safeguards.

  In determining what safeguards are reasonable for your organization, you will want to consider how sensitive the information is. *All* personal information should be protected from loss, theft, and inappropriate use or disclosure, but information like credit card numbers, Social Insurance Numbers, Alberta health care numbers, driver's license numbers and birth dates can be used to cause harm if they are lost or stolen.

Common sense security practices

- File cabinets should be locked when unattended. Computers should have password protection to limit access to files containing staff and clients' information. More sensitive information will require additional safeguards.
- Limit access to personal information. Only those staff who need access to the information should have a key to the file cabinet or know computer passwords.
- The best safeguard is to not collect or keep more information than you need.
- A guardian can request information on behalf of a dependent child or adult, or with the consent of another individual.
- Individuals have the right to request access to their own personal information held by your organization.
- When you respond to a request, inform the applicant of: whether you have a record of the information, whether you will give access to all or part of the record, and where, when, and how access will be given.