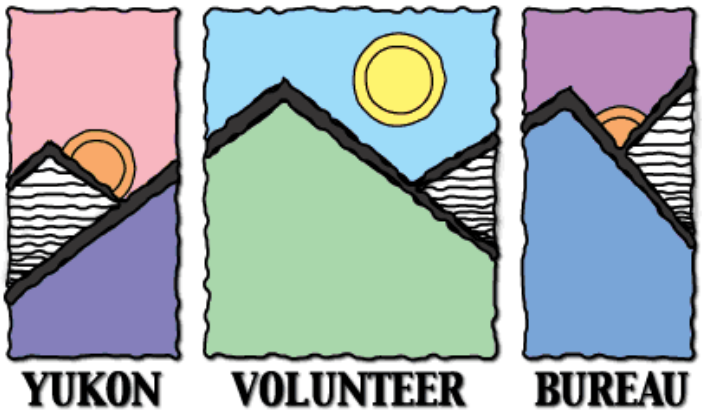

PRIVACY SELF-AUDIT OUTLINE

FOR NON-PROFIT ORGANIZATIONS

The following questions are based on 10 universal privacy protection principles. The principles are set out in the Canadian Standards Association (CSA) Model Privacy Code. They are also included in Schedule 1 of the *Personal Information Protection and Electronic Documents Act* (PIPEDA), the federal privacy protection legislation for business and organizations.

The purpose of this self-audit is twofold: to better understand why the organization collects personal information, and how personal privacy is protected by the organization's collection, use, disclosure, retention and destruction practices.

1. **What is the role and function of the organization?**

   It may be helpful to refer to the organization's mission statement and strategic plan to define the purpose for which the organization exists.

2. **What are its principle activities?**

   The main program activities should be listed, particularly those which involve the handling of personal information such as membership information, registration forms, etc.

3. **What privacy laws and regulations impact the organization?**

   Depending on the complexity of the organization, you may wish to get legal advice on this question. Personal information collected, used, or disclosed by non-profit organizations is normally not covered by Territorial or Federal Legislation. However, the personal information of employees (paid staff) of non-profit organizations may be covered by PIPEDA. Also, if a non-profit organization operates a gift shop or other commercial enterprise, the information collected in the course of commercial activity is covered by PIPEDA.

4. **What type of personal information does the organization collect?**

   You should refer to the principle activities of your organization (question 2, above), and identify the type of information that is currently being collected. These are commonly referred to as 'data elements', which include such things as name, age or date of birth, address, telephone number, height, weight, and any other information about an individual. Keep in mind that an important privacy principle is to only collect data elements that are necessary for the purpose(s) for which the information is collected.

5. **Does the organization have privacy policies and procedures with respect to collection, use, retention, disclosure, and destruction of personal information?**

   This question relates to some of essential privacy principles. Policy and procedures should address:

   a. *identifying the purpose for the collection of information;*
   b. *stating the purpose when the information is collected;*
   c. *determining the form of consent required for the collection, use, disclosure;*
   d. *collecting personal information directly from the individual the information is about, unless it is authorized in some other way;*
   e. *limiting the amount of personal information collected to that required for the purpose in a.;*
   f. *using the information only for the purpose in a.;*
   g. *disclosing or sharing the information only in ways that are consistent with the purpose in a.;*
   h. *obtaining further consent from the individual the information is about, if the information is to be shared in ways not consistent with the purpose in a.;*
   i. *retaining personal information only for the length of time necessary to meet the purpose for its collection – setting up a records destruction schedule; and*
   j. *determining the method of destruction for records or information no longer required.*

6. **Does the organization have responsibility and accountability assigned for managing a privacy program?**

   Someone in the organization should be assigned to manage the privacy program and be responsible for responding to questions or concerns about the collection, use, or disclosure of personal information. The 'privacy officer' should study and learn the privacy principles and their application; monitor adherence the principles, communicate the policies and practices when appropriate (perhaps through a website privacy policy statement, or in hardcopy form), and conduct scheduled privacy audits – annually at a minimum.

7. **Does the organization know where all personal information is stored?**

   A sound Information Management System is critical. Many organizations, particularly non-profits that rely on volunteer support, do not have a central records storage system. Although it may not be necessary to have all records centrally located, it is important to create an inventory of where the information is and how personal information in those records can be managed for privacy protection. This may be especially challenging when records are created and shared electronically.

8. **How is personal information protected from unauthorized access, use, disclosure, destruction?**

   This question refers to both physical security and information systems security. Premises where personal information is stored should have reasonable security measures in place to prevent unauthorized access. File cabinets containing sensitive personal information should be locked. Computers (workstations and laptops) should be password protected on startup, and files with personal information should be password protected or encrypted. Levels of sensitivity should be managed with 'need to know' login access. The use of laptops should be subject to a security policy.

9. **Is any personal information collected by the organization disclosed to third parties?**

   Disclosure of personal information to third parties should be consistent with the purposes for collection. If further disclosure is necessary, consent must be obtained unless the consent is implied by the nature of the activity, or if the disclosure is required by law.

10. **Are employees properly trained in handling privacy issues and concerns?**

    All staff should be familiar with the organization's privacy program. They should maintain vigilance to prevent the inadvertent improper disclosure of personal information. It may be useful to have employees sign, in addition to a confidentiality agreement, a Privacy Protection Agreement – one that acknowledges an understanding of the privacy policies and procedures, and what steps to take in the event of a privacy breach. Staff should know how to respond to complaints and concerns about privacy and where they can be referred for attention.

11. **Does the organization have adequate resources to develop, implement, and maintain an effective privacy program?**

    Resources would involve, at a minimum, the designation of a Privacy Officer for the organization. Further resource considerations would require an assessment of the organization's activities as they relate to the handling of personal information.

12. **Does the organization complete a periodic assessment to ensure that privacy policies and procedures are being followed?**

    As indicated in Q.6, the person designated as Privacy Officer should schedule periodic assessments dependent on the level of risk, but at least annually.

RESOURCES:

1. Institute of Internal Auditors

http://www.theiia.org/guidance/technology/gtag/gtag5/

Managing and Auditing Privacy Risks is intended to provide the chief audit executive (CAE), internal auditors, and management with insight into privacy risks that the organization should address when it collects, uses, retains, or discloses personal information. This guide provides an overview of key privacy frameworks which help to understand the basic concepts and aid in finding the right sources for more guidance regarding expectations and what works well in a variety of environments. It also covers the details on how internal auditors complete privacy assessments.

2. Privacy Commissioner of Canada

http://www.privcom.gc.ca/information/index_e.asp

Resource centre on the web site of the Privacy Commissioner of Canada. Includes a Privacy Protection Guide for individuals, and a Guide for organizations, as compliance tools under PIPEDA.

http://www.privcom.gc.ca/information/guide/2007/gl_070801_02_e.asp

Helpful information from the Privacy Commissioner's Office on the key steps an organization should take in responding to a privacy breach.

3. Canadian Standards Association (CSA)

http://www.csa.ca/standards/privacy/code/Default.asp?language=english

The Privacy Code from the CSA, outlining the 10 privacy principles and an appendix of the OECD Guidelines which form the basis for the CSA Privacy Code.

This outline was prepared in collaboration with Hank Moorlag, former Yukon Information & Privacy Commissioner, who now consults on Administrative Fairness and Fair Information Practices.

Hank's contribution of this outline was as a volunteer. He is available to member organizations for a one-hour consultation on Privacy Protection, as a follow-up to a self-audit at no cost.

He can be reached at Common Ground Consulting 633-3881 email: commonground@northwestel.net