A variety of federal, provincial and/or territorial privacy legislation is currently in place in Canada. As you consider developing a workplace policy, it will be important for you to know what privacy laws apply to your workplace and how your practices comply with and respect those laws. For a comprehensive list of federal, provincial and territorial privacy legislation in Canada please refer to the Office of the Privacy Commissioner of Canada website at: http://www.privcom.gc.ca/legislation/index_e.asp.

Privacy legislation deals with the collection, retention, use and disclosure of:

- Personal information about individual customers, donors or members of the public
- Personal health information
- Personal information and/or personal health information pertaining to an employee, in other words, the privacy and confidentiality of employee records in the workplace

Personal information is any information about an identifiable individual whether recorded or not. Organizations can only collect personal information that is appropriate for the specific transaction and they must explain why they need the information, what it will be used for, and whether they plan to disclose it to anyone else. They must also obtain consent for this use and disclosure. Personal health information is information that identifies an individual and that relates to the physical or mental health of an individual, including the provision of health care.

For the purposes of this information sheet employee records and personnel files in the workplace and workplace privacy practices will be highlighted.

Employee privacy and confidentiality is currently protected by a variety of legislation, including for example: employment standards, collective agreements and human rights laws. Specific privacy legislation may also, in some cases, apply to personal health information that is gathered and stored in the personnel file.

Many employers have been monitoring developments with privacy legislation in Canada and what it means for them and their employees. Although some privacy laws may not yet apply to the not-for-profit/NGO sector, many employers have been reviewing workplace practices with respect to how personnel files are maintained and how personal information and/or personal health information is gathered and stored. Many employers are developing privacy and confidentiality workplace policies that provide employers and employees with specific details about how their information is gathered and handled.

The following list provides some examples of recommended practices that employers can use as a guideline when reviewing workplace privacy policies and practices. This list is by no means exhaustive.
1. Appoint a person or a working group responsible for developing and monitoring the privacy policy and activities within the organization.

2. Conduct a privacy audit (see page 2) and audit how personnel records are stored and maintained. Be sure to include current employees, recent departures and archived records.

3. Establish organizational standards for all managers to follow consistently (for example what information is provided to a financial institution when they call to verify employment and income information, how are requests for reference checks or for address/telephone numbers of a former employee handled?)

4. Review all organizational forms that call for the collection of personal information to ensure they are limited to only required details. Include a privacy statement on each form detailing the reason for the information and how it will be used. The forms may include, but are not limited to: application forms, interview templates, new hire information forms, group insurance applications including short and long term disability applications, human resource information system data collection, financial and/or payroll related forms, discipline records, performance appraisals.

5. Develop a statement of consent to the collection, use and disclosure of employee personal information. One option is for each employee to sign the consent when hired. Information and consent details should also be included in the organizational privacy policy.

6. Develop an access to information policy advising employees they are permitted to access their personnel file. Highlight in the policy any specific procedures to be followed (for example: nothing to be removed or altered, a person representing the employer must be present).

7. Keep all files containing medical and/or personal health information separate from regular employee personnel and/or other administrative files. All files must be stored securely at all times, preferably in a central location.

8. Know who has access to personal information at all times. Ensure that anyone with clerical/filing responsibilities is restricted in terms of access to information.

9. Anyone with access to personal information and/or personal health information must sign a confidentiality agreement, subject to disciplinary action if breached.

10. Complimentary policies including, but not limited to: e-mail, internet use, computer systems and confidentiality should be developed and implemented.

11. A compliance and complaint procedure should be established and monitored regularly.

12. When lawfully disclosing any information to a third party, ensure that only the specific information required is provided to the third party. In other words data should be stored and/or provided in a form that permits retrieval and disclosure of only those portions that would be required.

13. Provide a written description of the practices you use to protect personal information, and the name of the person in your organization to contact if you have any questions or concerns.

If specific privacy legislation does not yet apply to your organization, learning about and implementing recommended practices around privacy in the workplace will ensure that you are well-prepared as well as in compliance with employment and/or human rights legislation.

Objective of a Privacy Audit

A systematic review of the organization's personal information holdings and handling practices to create an organized inventory of personal information.
Why Conduct a Privacy Audit

• To provide the specific information required when developing a customized privacy policy.

• To identify potential gaps in privacy compliance.

• To identify areas of risk to the employer or the employee.

• To provide all employees with clear procedures that must be followed.

Suggestions for Questions - Departmental Privacy Audit Form

• What personal information does your department have?

• What are the purposes for collecting the personal information?

• How do you use the personal information?

• How long do you retain the personal information and why?

• How do you store the personal information?

• What format is the personal information in? Paper? Electronic?

• To whom do you disclose the personal information and why?