IMPLEMENTING PIPEDA QUESTIONNAIRE

The following are some common sense questions you can use to help your organization implement PIPEDA. Not all of the following questions will apply to all organizations, as the Act applies to a wide variety and size of organizations. Consider each question along with your organization's current practices. Answering "no" indicates areas that need to be addressed or improved.

QUESTION	YES	NO
PERSONAL INFORMATION HOLDING		
Does your Association know what personal information is?		
Does your Association collect, use or disclose personal information in your day-to-day activities?		
Does your Association have an inventory of your personal information holdings?		
Does your Association know where personal information is held (physical locations and files)?		
Does your Association know in what format(s) the personal information is kept (electronic, paper, etc.)?		
Does your Association know who has access to personal information in and outside your organization?		
ACCOUNTABILITY OF ORGANIZATION AND STAFF		
Has your Association named a privacy officer who is responsible for your organization's overall compliance with the Act?		
Is this responsibility shared with more than one person?		
If these responsibilities are shared, have they been clearly identified?		
Can your privacy officer respond to internal and external privacy questions on behalf of the organization, or do they know who should respond?		
Does your Association know who receives and responds to:		
requests for personal information?		
requests for correction?		
complaints from the public?		
Do your members know whom to contact:		
for general inquiries regarding their personal information?		
to request their personal information?		
to request corrections to their personal information?		
for complaints?		
Is your privacy officer able to explain to your members the steps and procedures for requesting personal information and filing complaints?		
Has your Association been trained on the Act?		
Will there be ongoing training?		
Is your Association able to explain the purposes for the collection, use and disclosure of personal information to members in easy to understand terms?		
Is your Association able to explain to other volunteers when and how they may withdraw consent and what the consequences, if any, there are of such a withdrawal? internal		

QUESTION	YES	NO
reviews, public complaints and decisions of the courts?		
INFORMATION FOR CUSTOMERS AND EMPLOYEES		
Will you inform your volunteers of new privacy issues raised by technological changes?		
Do you have documents that explain your personal information practices and procedures to your members?		
Does this information include how to:		
obtain personal information?		
correct personal information?		
make an inquiry or complaint?		
Does this information describe personal information that is:		
held by the organization and how it is used?		
disclosed to subsidiaries and other third parties?		
Is the privacy policy prominent and easy to find? Is it easily understandable?		
Does your Association have a privacy policy for the Association Web site?		
Does the Association's application forms. Questionnaires, survey forms, pamphlets and brochures clearly state the purposes for the collection, use or disclosure of personal information?		
Has your Association reviewed all your public information material to ensure that any sections concerning personal information are clear and understandable?		
Has your Association ensure that the public can obtain this information easily and without cost?		
Is this information reviewed regularly to ensure that it is accurate, complete and up to date?		
Does this information include the current name or title of the person who is responsible for overseeing compliance with the Act?		
LIMITING COLLECTION, USE, DISCLOSURE AND RETENTION TO IDENTIFIED PURPOSES		
Has your Association identified the purposes for collecting personal information?		
Are these purposes identified at or before the time the information is collected?		
Does your Association collect only the personal information needed for identified purposes?		
Does your Association document the purposes for which personal information is collected?		
If your Association gathers and combines personal information from more than one source, does it ensure that the original purposes have not changed?		
Has your Association developed a timetable for retaining and disposing of personal information?		
When your Association no longer require personal information for the identified purposes or it is no longer required by law, does your Association destroy, erase or make it anonymous?		
CONSENT		
Does your Association know that an individual's consent must be obtained before or at the time they collect personal information?		
Does your Association know they must obtain an individual's consent before any new use or new disclosure of the information?		
Does your Association use express consent whenever possible, and in all cases where the information is sensitive or the individual would reasonably expect it?		

QUESTION	YES	NO
Is your Association's consent statement worded clearly, so that an individual can understand the purpose of the collection, use or disclosure?		
Does your Association make it clear to volunteers that they need not provide personal information that is not essential to the purpose of the collection, use or disclosure?		
THIRD PARTY TRANSFERS		
Does your Association use contracts to ensure the protection of personal information transferred to a third party for processing?		
Does the contract limit the third party's use of information to purposes necessary to fulfill The contract?		
Does the contract require the third party to refer any requests for access or complaints about the information transferred to you?		
Does the contract specify how and when a third party is to dispose of or return any personal information it receives?		
ENSURING ACCURACY		
Is personal information sufficiently accurate, complete and up to date to minimize the possibility that your organization might use inappropriate information?		
Does your Association document when and how personal information is updated, to ensure its accuracy?		
Does your Association ensure that personal information received from a third party is accurate and complete?		
SAFEGUARDS		
Has your Association reviewed your physical, technological and organizational security measures?		
Do they prevent improper access, modification, collection, use, disclosure and/or disposal of personal information?		
Is personal information protected by security safeguards that are appropriate to the:		
sensitivity of the information?		
scale of distribution?		
format of the information?		
method of storage?		
Has your Association developed a "need-to-know" test to limit access to personal information to what is necessary to perform assigned functions?		
Has your Association been trained about security practices to protect personal information?		
For example, are volunteers aware that personal information should not be left displayed on their computer screens or desktops?		
Is your Association aware that they should properly identify individuals and establish their tight to access the personal information before disclosing it?		
Does your Association have rules about who is permitted to add, change or delete personal information?		
Is there a records management system that assigns user accounts, access rights and security authorizations?		
Does your Association ensure that no unauthorized parties may dispose of, obtain access to modify or destroy personal information?		
REQUESTS FOR ACCESS TO PERSONAL INFORMATION		
Is your Association aware of the time limits the law allows to respond to access		

QUESTION	YES	NO
requests?		
Can your Association retrieve personal information to respond to individual access requests with a minimal disruption to operations?		
Does your Association's information system facilitate the retrieval and accurate reporting ofan individual's personal information, including disclosures to third party organizations?		
Does your Association provide personal information to the individual at minimal or no cost?		
Does your Association advise requesters of costs, if any, before personal information is retrieved?		
Does your Association record an individual's response to being notified of the cost of retrieving personal information?		
Does your Association provide personal information in a form that is generally understandable? (For example, do you explain abbreviations?)		
Does your Association have procedures for responding to requests for personal information in an alternate format (such as Braille or audiotapes)?		
HANDLING COMPLAINTS		
Can an individual easily find out how to file a complaint with your Association?		
Does your Association deal with complaints in a timely fashion?		
Does your Association investigate all complaints received?		
Is your Association able to distinguish a complaint under the law from a general inquiry? If unsure, do they discuss this with the individual?		
Does your Association advise individuals about all available avenues of complaint, including the Privacy Commissioner of Canada?		
Are your Association's responses to public inquiries, requests and complaints reviewed to ensure they are handled fairly, accurately and quickly?		
When a complaint is found to be justified, does your Association take appropriate corrective measures, such as amending your policies and advising other Association members of the outcome?		