

ONTARIO PROFESSIONAL FORESTERS ASSOCIATION

PRIVACY CODE

April 2003

INTRODUCTION

The Ontario Professional Foresters Association (OPFA) recognizes that your right to privacy is an important issue. We understand your interest in maintaining your anonymity and protecting your private information while participating as a member of the OPFA. As a result, the OPFA manages your personal information with great care as reflected through this privacy policy.

While the OPFA has always tried to ensure your personal information was protected, this new privacy policy provides you with all of the safeguards as standardized in the Personal Information Protection and Electronic Documents Act. This recent piece of federal legislation is the first step to formally protecting your interests.

PRIVACY PROTECTION IN CANADA

This privacy policy has been developed to meet the compliance standards established by Canada's *Personal Information Protection and Electronic Documents Act*, the *CSA Model for the Protection of Personal Privacy* and *OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.

Personal Information Protection and Electronic Documents Act

The *Personal Information Protection and Electronic Documents Act*, formerly referred to as Bill C-6 is essentially about balance. On one hand, it respects an individual's right to privacy while on the other, it recognizes the need for industry and organizations to collect, use and disclose personal information. This law as its name suggests, encompasses two primary objectives. The first objective is to establish rules that govern the collection, use and disclosure of personal information by private sector organizations. The second objective is to acknowledge the validity and legality of electronic documents.

This federal law will significantly impact the way private businesses, corporations, federal agencies, not-for-profit organizations and associations handle the personal information with which they have been entrusted. At the same time, it will clearly establish a code of privacy practices that will provide Canadians from coast to coast with a mechanism to ensure their personal information is handled respectfully.

The heart of this Act is based on the Ten Principles established by the Canadian Standards Association's *Model Code for the Protection of Personal Information*. These principles were recognized as a Canadian standard in 1996 and address the ways in which organizations should collect, use and disclose personal information. They also address an individual's right to access his/her personal information in addition to his/her right to have it amended where appropriate.

In order to govern the commercial information-handling practices within provincial jurisdictions, each province has been encouraged to enact legislation that is substantially similar to the federal law. Quebec enacted comparable legislation in 1994 called an *Act Respecting the Protection of Personal Information in the Private Sector*. As other provinces enact similar legislation, organizations conducting commercial activity within a province will be subject to the provisions of their provincial laws rather than the federal Act. However, the *Personal Information Protection and Electronic Documents Act* will continue to regulate cross-border, inter-provincial and international trade and commerce.

The implementation of this federal law relating to privacy will occur in three stages. The first phase, which is effective as of January 1, 2001 will affect federally-regulated private organizations including Canadian banks and airlines as well as to organizations that collect, use or disclose personal information for profit on an inter-provincial or international basis. On January 1, 2002, this law will be extended to cover personal health information. Two years later on January 1, 2004, most organizations regardless of their size, which collect, use or disclose personal information in the course of commercial activity, will become subject to the provisions of this Act.

For more information regarding this legislation, please visit the official Web site of the [Privacy Commissioner of Canada](#) or the [Electronic Commerce branch of Industry Canada](#).

SCOPE

OPFA policy applies to personal information about identifiable OPFA members that is collected, used or disclosed by the OPFA. It also applies to the management of personal information in any form whether oral, electronic or written.

GENERAL APPLICATION

The policy will apply to and protect all personal information collected used or disclosed by the OPFA, **except information that is aggregated in such a manner that it cannot be connected to a person and/or information which is publicly listed in a written or online directory or typically made available through directory assistance as permitted by law.**

Personal information may be collected when a person applies for membership in the OPFA or registers for OPFA sponsored events (e.g. Annual General Meeting, Continuing Education Seminars). It may also be collected when: a person makes any inquiries by telephone, signs a contract, registers or provides information by email or through the Internet, inquires about processes, procedures, policies and interpretation of professional standards, or when he/she makes a complaint.

However, the policy **does not** impose any limits on the collection, use or disclosure of the following information:

- a) a person's name, address, telephone number and electronic address, when listed in a directory or available through directory assistance;
- b) an employee's name, title, business address (including email address) and phone and fax numbers; or
- c) information that is publicly available and is specified by regulation pursuant to the Personal Information Protection and Electronic Documents Act.

GUIDELINES FOR INTERNET/WEBSITE USERS

In some cases, users' **non-personal** information and data may be automatically collected through the standard operation of the OPFA's internet server or through the use of "cookies". "Cookies" are small text files that are used by websites to: (a) recognize repeat users; (b) track usage behavior; and (c) compile aggregate data that will permit content improvements and targeted advertising. The OPFA cannot control or prevent the use of cookies or any information obtained through such cookies by advertisers or third parties. If you do not want information collected through the use of cookies, most browsers permit you to disable the cookie feature. However, cookies may be required for the use of certain features on our Website.

Any submissions made to discussion areas or other public areas on the OPFA's website are done so with a user's understanding that they are accessible to third parties. If comments are not intended for third parties, you are advised not to make any submissions.

The OPFA policy generally and in connection with Internet use is subject to the requirements or provisions of any applicable legislation, regulations or agreements, or order of any court, or other lawful authority.

THE PRIVACY PRINCIPLES THE OPFA FOLLOWS

There are ten principles that form the basis of the OPFA's policy. These principles are interrelated and the OPFA shall adhere to them as a whole. Each principle must be read in conjunction with the accompanying commentary. As

permitted by *the Personal Information Protection and Electronic Documents Act*, and its regulations, the commentary in the OPFA's policy may be tailored to reflect personal information issues specific to the OPFA.

To better understand the policy, the OPFA has set out some basic definitions to use when reading and interpreting the principles below:

Collection - the act of gathering, acquiring, recording, or obtaining personal information from any source, including third parties, by any means.

Consent - voluntary agreement with the collection, use and disclosure of personal information for defined purposes. Consent can be either express or implied and can be provided directly by the individual or by an authorized representative. Express consent can be given orally, electronically or in writing, but is always unequivocal and does not require any inference on the part of the OPFA. Implied consent is consent that can reasonably be inferred from an individual's action or inaction.

Member - an individual who is or is in the process of becoming a member in the Ontario professional Foresters Association.

Disclosure - making personal information available to a third party.

Personal information - information about an identifiable individual that is recorded in any form, **but does not include** aggregated information that cannot be associated with a specific member. For a member, such information does not include information that is aggregated in such a manner that it cannot be connected to him/her and/or information which is publicly listed in a written or online directory or typically made available through directory assistance.

Third party - an individual or organization outside the OPFA.

Use - the treatment, handling, and management of personal information by and within the OPFA

PRIVACY PRINCIPLES

The Ontario Professional Foresters Association (OPFA) has always been and will continue to be, committed to maintaining the accuracy, confidentiality, and security of your personal and financial information. As part of this commitment, the Association has established Ten Privacy Principles to govern its actions as they relate to the use of member information. The OPFA invites you to review their principles, which have been built upon the values set by the Canadian Standards Association's *Model Code for the Protection of Personal Information* and Canada's *Personal Information Protection and Electronic Documents Act*.

[Principle 1 - Accountability](#)

[Principle 2 - Identifying Purposes](#)

[Principle 3 - Consent](#)

[Principle 4 - Limiting Collection](#)

[Principle 5 - Limiting Use, Disclosure and Retention](#)

[Principle 6 - Accuracy](#)

[Principle 7 - Safeguarding Customer Information](#)

[Principle 8 - Openness](#)

[Principle 9 - Customer Access](#)

[Principle 10 - Handling Customer Complaints and Suggestions](#)

Principle 1 – Accountability

The Ontario Professional Foresters Association is responsible for maintaining and protecting the member information under its control. In fulfilling this mandate and is required to designate an individual or individuals who is accountable for ensuring compliance with the Ten Privacy Principles.

- 1.1 The Registrar is the person designated as being accountable for compliance with these principles. The Office Manager has the delegated by the Registrar to take responsibility for the day-to-day collection and processing of personal information.
- 1.2 The OPFA is responsible for the personal information in its possession or control.
- 1.3 The OPFA shall implement policies and practices to give effect to these principles, including:
 - implementing procedures to protect personal information and to oversee the OPFA' s compliance with its policy;
 - establishing procedures to receive and respond to inquiries or complaints;
 - training and communicating to staff about OPFA policies and practices; and
 - developing public information to explain the OPFA's policies and practices.

Principle 2 - Identifying Purposes

The purposes for which member information is collected shall be identified before or at the time the information is collected.

- 2.1 The OPFA collects personal information only for the following reasons:

- to establish and maintain ongoing business relations with members
 - to understand member needs
 - to develop, enhance, market or provide products and services
- 2.2 The OPFA shall specify orally, electronically or in writing the identified purposes to the member or employee at or before the time personal information is collected. Upon request, persons collecting personal information shall explain these identified purposes or refer the individual to a designated person within the OPFA who shall explain the purposes.
- 2.3 Unless required by law, the OPFA shall not use or disclose for any new purpose, personal information that has been collected without first identifying and documenting the new purpose and obtaining the consent of the member.

Principle 3 – Consent

The knowledge and consent of the member are required for the collection, use or disclosure of member information except where required or permitted by law.

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 a member 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.

- 3.1 In obtaining consent, the OPFA shall use reasonable efforts to ensure that a member is advised of the identified purposes for which personal information collected will be used or disclosed. Purposes shall be stated in a manner that can be reasonably understood by the member or employee. (See Principle 2)
- 3.2 Generally, the OPFA shall seek consent to use and disclose personal information at the same time it collects the information. However, the OPFA may seek consent to use and disclose personal information after it has been collected, but before it is used or disclosed for a new purpose.

- 3.3 The OPFA **will** only require members to consent to the collection, use or disclosure of personal information as a condition to the supply of a product or service if such collection, use or disclosure is required to fulfill the identified purposes. (See Principle 2).
- 3.4 In determining the appropriate form of consent, the OPFA shall take into account the sensitivity of the personal information and the reasonable expectations of its members.
- 3.5 In general, the use of products and services by a member or visitor to a Website constitutes implied consent for the OPFA to collect, use and disclose personal information for all identified purposes. For sensitive information, the OPFA will obtain express consent at or before the time of collection.
- 3.6 A member may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. (See Principle 3). Members may contact the OPFA at the address below for more information regarding the implications of doing so. (See Principle 1).

Principle 4 - Limiting Collection

The member information collected must be limited to those details necessary for the purposes identified by the OPFA. Information must be collected by fair and lawful means.

- 4.1 The OPFA collects personal information primarily from its members.
- 4.2 The OPFA may also collect personal information from other sources including but not limited to credit bureaus or other third parties who represent that they have the right to disclose the information.

Principle 5 - Limiting Use, Disclosure and Retention

Member information may only be used or disclosed for the purpose for which it was collected unless the member has otherwise consented, or when it is required or permitted by law. Member information may only be retained for the period of time required to fulfill the purpose for which it was collected.

- 5.1 The OPFA may disclose a customer's personal information to:
 - another professional foresters association;
 - a company or individual employed by the OPFA to perform functions on its behalf, such as data processing;

- an agent or third party retained by the OPFA in connection with OPFA administration or the provision of the OPFA's products or services
 - a public authority or agent of a public authority, if in the reasonable judgment of the OPFA, it appears that there is imminent danger to life or property which could be avoided or minimized by disclosure of this information;
 - a person who, in the reasonable judgment of the OPFA, is seeking the information as an agent of the member; and
 - a third party or parties, where the member consents to such disclosure or disclosure is required by law or emergency.
- 5.2 Except as permitted in this Principle, the OPFA does not provide or sell its customer lists to any outside company for use in marketing or solicitation.
- 5.3 Only OPFA employees with a business need to know, or whose duties reasonably so require, are granted access to personal information about members.
- 5.4 The OPFA shall keep personal information only as long as it remains necessary or relevant for the identified purposes or as required by law. Depending on the circumstances, where personal information has been used to make a decision about a member, the OPFA shall retain, for a period of time that is reasonably sufficient to allow for access by the member, either the actual information or the rationale for making the decision.
- 5.5 Personal information that is no longer necessary or relevant for the identified purposes or required to be retained by law shall be destroyed, erased or made anonymous. In any event, the OPFA shall maintain reasonable and systematic controls, schedules and practices for such information, its retention and destruction.

Principle 6 – Accuracy

Member information must be maintained in as accurate, complete and up-to-date form as is necessary to fulfill the purposes for which it is to be used.

- 6.1 Personal information used by the OPFA shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about a member.

- 6.2 The OPFA shall update personal information about members as and when necessary to fulfill the identified purposes or upon notification by the individual.

Principle 7 - Safeguarding Customer Information

Member information must be protected by security safeguards that are appropriate to the sensitivity level of the information.

- 7.1 The OPFA shall protect personal information against such risks as loss or theft, unauthorized access, disclosure, copying, use, modification or destruction, through appropriate security measures. The OPFA shall protect the information regardless of the format in which it is held.
- 7.2 The OPFA shall protect personal information it discloses to third parties by contractual agreements stipulating the confidentiality of the information and the purposes for which it is to be used.
- 7.3 All of the OPFA's employees with access to personal information shall be required as a condition of employment to contractually respect the confidentiality of personal information.

Principle 8 – Openness

The OPFA shall make readily available to members and employees specific information about its policies and practices relating to the management of personal information.

- 8.1 The OPFA shall make information about its policies and practices easy to understand, including:
- the title and address of the person or persons accountable for the OPFA's compliance with the policy and to whom inquiries or complaints can be forwarded;
 - the means of gaining access to personal information held by the OPFA; and
 - a description of the type of personal information held by the OPFA, including a general account of its use.
- 8.2 The OPFA shall make information available to help members exercise choices regarding the use of their personal information and the privacy-enhancing services available from the OPFA.

Principle 9 - Member Access

Upon request, a member shall be informed of the existence, use and disclosure of their information, and shall be given access to it. Members may verify the accuracy and completeness of their information, and may request that it be amended, if appropriate.

NOTE: In certain situations, the OPFA may not be able to provide access to all of the personal information it holds about a member. 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, information that is subject to solicitor-client or litigation privilege, or, in certain circumstances, information of a medical nature. The OPFA shall provide the reasons for denying access upon request.

- 9.1 Upon request, the OPFA shall afford members a reasonable opportunity to review the personal information in the individual's file. Personal information shall be provided in understandable form within a reasonable time, and at a minimal or no cost to the individual.
- 9.2 Upon request, the OPFA shall provide an account of the use and disclosure of personal information and, where reasonably possible, shall state the source of the information. In providing an account of disclosure, the OPFA shall provide a list of organizations to which it may have disclosed personal information about the individual when it is not possible to provide an actual list.
- 9.3 In order to safeguard personal information, a member may be required to provide sufficient identification information to permit the OPFA to account for the existence, use and disclosure of personal information and to authorize access to the individual's file. Any such information shall be used only for this purpose.
- 9.4 The OPFA shall promptly correct or complete any personal information found to be inaccurate or incomplete. Any unresolved differences as to accuracy or completeness shall be noted in the individual's file. Where appropriate, the OPFA shall transmit to third parties having access to the personal information in question any amended information or the existence of any unresolved differences.
- 9.5.1 Members can obtain information or seek access to their individual files by contacting the designated representative at the OPFA's business office as described below.

Principle 10 – Handling member Complaints and Suggestions

Members may direct any questions or enquires with respect to the privacy principles outlined above or about our practices by contacting the designated person(s) accountable for privacy in the OPFA.

- 10.1 The OPFA shall maintain procedures for addressing and responding to all inquiries or complaints from its members about the OPFA's handling of personal information.
- 10.2 The OPFA shall inform its members about the existence of these procedures as well as the availability of complaint procedures.
- 10.3 The person or persons accountable for compliance with the OPFA's policy may seek external advice where appropriate before providing a final response to individual complaints.
- 10.4 The OPFA shall investigate all complaints concerning compliance with the policy. If a complaint is found to be justified, the OPFA shall take appropriate measures to resolve the complaint including, if necessary, amending its policies and procedures.

HOW YOU CAN PROTECT YOUR INFORMATION

The OPFA does its best to protect and safeguard your personal information, but there are measures you should take as well. The following is a list of things you can do to protect yourself against fraud and uninvited intrusion.

Passwords

Passwords can be used to identify you and authenticate your permission to access personal information. When you enroll in online services, ensure that the passwords you use are encrypted. [Encryption](#) is presently the most effective way to achieve data security. Just as it is important for the OPFA to employ strict procedures to safeguard your personal information, you also should take precautions in handling your passwords. When selecting a password, it is suggested that you use a combination of letters and numbers and do not use words that can be easily associated with you such as the name of a family member, a pet or the street on which you live. It is also suggested that you change your password regularly.

Personal Information

You should not share personal information such as your Personal Identification Number, Social Insurance Number or credit card number with others unless you

clearly understand the purpose of their request and you know with whom you are dealing.

Online Security

To make sure your connection to the protected areas of some websites are secured, look for either a 'closed lock' or an 'unbroken key' icon located at the bottom right hand side of your browser's task bar. You may also check the address bar to determine if [SSL](#) (Secure Socket Layer) is active by looking at the beginning of the address. If it starts with "https" rather than the standard "http", then SSL is operating.

Suspicious Solicitation

From time to time, the OPFA will seek information and/or opinion via telephone, mail and e-mail. If you are unsure that the information you are receiving is from the OPFA , please call us at 1-705-436-2226 to verify legitimacy.

FOR MORE INFORMATION:

Please contact the OPFA directly as follows by:

E-mail: opfa@on.aibn.com

Telephone: 1-705-436-2226

Mail:

The Ontario Professional Foresters Association
8000 Yonge Street, Unit 3
Innisfil, Ontario
L9S 1L5

You can also obtain more information as well as a copy of the federal legislation through the Privacy Commissioner of Canada's web site at www.privcom.gc.ca.