



## CAIP PRIVACY CODE

*Since January 1, 2004 the Government of Canada has required all businesses and organizations that collect, use and disclose personal information in the normal course of business to establish and post a Privacy Policy. CAIP's Privacy Code is a guide to assist members in establishing their own Privacy Policy. We strongly recommend members seek the advice of a lawyer in ensuring their Privacy Policy meets the requirements of the Personal Information Protection and Electronic Documents Act (PIPEDA)*

### Contents

- Purpose of the CAIP Privacy Code
- Scope and Application
- Definitions
- The Ten Privacy Principles

### Purpose of the CAIP Privacy Code

In October 1996, CAIP released its voluntary Code of Conduct which stated that privacy was of fundamental importance to its members and that they would respect and protect the privacy of their users and would disclose personal information to law enforcement authorities only as required by law.

CAIP supports industry self-regulatory efforts in several areas, including privacy. The CAIP Privacy Code is based on the Canadian Standards Association Model Code for the Protection of Personal Information, CAN/CSA-Q830-96 (the "CSA Code"), which was published as a National Standard of Canada and which forms the basis for the new Personal Information Protection and Electronic Documents Act. CAIP has attempted to apply the principles of the CSA Code specifically to the online environment in developing its own CAIP Privacy Code.

CAIP will continue to review the CAIP Privacy Code (the "Code") every couple of years to make sure it is relevant and remains current with changing technologies, current regulatory regimes and the evolving needs of its members and their users.

### Scope and Application

The CAIP Privacy Code is a voluntary code that represents a formal statement of principles and guidelines concerning the minimum protection that CAIP members will provide to their users regarding the protection of personal information.

The Code applies to the management of personal information about a member's users in any form whether oral, electronic or written that is collected, used or disclosed by the member.

This model is intended to help members develop their own privacy code and policies. The Code consists of ten principles that are closely related. Where a member chooses to adopt the principles of the CAIP Privacy Code, the member undertakes to follow all ten principles.

In addition, a member may define how it subscribes to each principle, modify details to provide specific examples, and include additional measures for the protection of privacy.

## Definitions

Because the following words have specific meanings, they have been defined at the beginning of the Code.

*clickstream data* - data derived from a user's navigational choices expressed during the course of visiting a World Wide Web site or other online areas.

*collect* - to gather, acquire, record or obtain personal information, from any source, by any means.

*consent* - voluntary agreement with the collection, use and disclosure of personal information. Consent can be express or implied, and provided directly by the user or through an authorized representative.

Express consent can be given orally, electronically or in writing, but is always unequivocal and does not require any inference by the member seeking consent. Members are encouraged to rely primarily on electronic or written consent given the uncertainties inherent in oral consent. Implied consent arises where consent may reasonably be inferred from the action or inaction of the user.

*disclose* - to make personal information available outside the member to a third party.

*Member* - an individual, organization or entity that belongs to CAIP and agrees to adhere to the CAIP Privacy Code. Each member may further tailor the CAIP Privacy Code and define clearly what affiliates, if any, are included in its definition of "the member" and bound by its code.

At the present time, adherence to the CAIP Code is not a mandatory requirement of becoming and remaining a CAIP member. CAIP members are strongly encouraged to implement this Code as it will become mandatory through legislative initiatives at the provincial and federal level.

*personal information* - information about a user, but not aggregated information that cannot be associated with a specific user.

Personal information includes but is not limited to information such as a user's name, postal and electronic addresses, age, gender, income, employment, credit information, billing records, and the like. Clickstream data is only considered personal information if it is linked to other personal information about a user.

*third party* - an individual or organization outside the member.

*use* - to manage personal information by and within the member.

*user* - an individual who uses, or applies to use, a member's products or services, or who corresponds with a member

## **The Ten Privacy Principles**

- Principle 1 - Accountability
- Principle 2 - Identifying purposes of personal information
- Principle 3 - Getting consent
- Principle 4 - Limits for collecting personal information
- Principle 5 - Limits for using, disclosing and keeping personal information
- Principle 6 - Keeping personal information accurate
- Principle 7 - Safeguarding personal information
- Principle 8 - Making information about policies and procedures available to users
- Principle 9 - User access to personal information
- Principle 10 - Handling complaints and questions

The following ten principles seek to balance the application of information age technologies with the privacy concerns of users.

### **1. Accountability**

Members are responsible for personal information under their control.

Members are also responsible for any personal information transferred to third parties for processing on their behalf and should use contractual or other means to provide a comparable level of protection.

Members will designate one or more persons to be accountable for compliance with these principles.

Members will identify internally the person, or persons, to be accountable for compliance. Members will identify to users a method to contact such person or persons. Depending on the size of the organization, other individuals within the member may act on behalf of the designated person or take responsibility for the day-to-day collection and management of personal information.

Members will establish necessary policies and procedures to implement and comply with their own privacy codes, such as procedures for the collection, handling, storage and destruction of personal information, to train staff and to deal with complaints and to explain the member's policies and practices.

### **2. Identifying the purposes for collection of personal information**

Members will identify the purposes of collecting personal information, before or at the time the information is collected.

Members may collect personal information for any specified purpose. Generally, members collect personal information for the following purposes:

- i) to establish and maintain responsible commercial relations with users and to provide ongoing service;
- ii) to understand user needs;
- iii) to develop, enhance, market or provide products and services;
- iv) to manage and develop the member's business and operations; and
- v) to meet legal and regulatory requirements.

Members will identify their purposes for the collection, use and disclosure of personal information electronically, in writing or orally, and in language that users can easily understand.

Members will not use or disclose personal information for any new purpose beyond that for which it was originally collected without first identifying and documenting the new purpose and getting the user's consent.

### **3. Getting the user's consent**

The knowledge and consent of the user are required for the collection, use or disclosure of personal information, except where inappropriate.

In certain circumstances, however, members may collect, use or disclose personal information without the user's knowledge and consent., for example:

- when it is clearly in the interest of the user and consent cannot be obtained in a timely way, such as in a medical emergency;
- when the life, health or security of another individual is threatened;
- if seeking consent might defeat the purpose, such as for the investigation of a breach of an agreement or law;
- when disclosure is to the member's lawyer, to collect a debt, to comply with a court order, or as may otherwise be required by law.

Members will use reasonable efforts to inform users how the personal information collected will be used and disclosed.

Generally, a member will seek consent to use and disclose personal information at the same time it collects it. Sometimes, however, a member may identify a new purpose and seek consent to use and disclose personal information after it has been collected.

A user's consent can be express, implied, or given through an authorized representative. In determining the appropriate form of consent, the member will take into account the sensitivity of the information and the reasonable expectations of a user.

Members will provide full and fair disclosure of its collection use and disclosure pursuant to these principles and will not deceive a user into giving consent.

A user can withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. Members should inform users of the implications of withdrawing consent and how to do so.

### **4. Limits for collecting personal information**

Members will collect only the amount and type of personal information needed for the purposes they have identified.

Members will collect personal information using procedures that are fair and lawful.

When a member collects clickstream data that will be linked with other personal information about a user, the member will advise users what information is being collected and how it will be used. Otherwise, the collection, use or disclosure of clickstream data is not restricted.

Although a member will collect personal information primarily from users, it may also collect personal information from other sources including credit bureaus, or other third parties that represent that they have the right to disclose the information.

## **5. Limits for using, disclosing, and keeping personal information**

Members will use or disclose personal information only for the purposes it was collected, unless a user gives consent or as required by law.

A member may disclose personal information without consent when required to do so by law, e.g. subpoenas, search warrants, other court and government orders, or demands from other parties who have a legal right to personal information, or to protect the security and integrity of its network or system. In such circumstances, a member will protect the interests of its users by making sure that:

- i) orders or demands appear to comply with the laws under which they were issued; and
- ii) it discloses only the personal information that is legally required, and nothing more.

A member may notify users that an order has been received, if the law allows it.

Only a member's employees with a business need to know, or whose duties so require, should be granted access to users' personal information.

Members will keep personal information only as long as necessary to fulfill the identified purposes.

Depending on the circumstances, personal information used to make a decision about a user, such as when a user's account has been rejected, should be kept long enough to allow the user access to the information after the decision has been made.

Members will keep reasonable controls, schedules and practices for information and records retention, and will destroy, erase or make anonymous within a reasonable period of time any personal information no longer needed for its identified purposes or for legal requirements.

## **6. Keeping personal information accurate**

Members will keep personal information as accurate, complete and up-to-date as necessary for the purposes for which it is to be used

Members may rely exclusively on the representations provided by their users in determining the completeness, accuracy, and timeliness of the personal information. This Principle does not imply any obligation on the member to seek independent verification of any personal information supplied by the user.

## **7. Safeguarding personal information**

Members will protect personal information with safeguards appropriate to the sensitivity of the information.

Members will use appropriate safeguards to protect personal information against such risks as loss or theft, unauthorized access, disclosure, copying, use, modification or destruction.

## **8. Making information about policies and procedures available to users**

Members will be open about the policies and procedures they use to manage personal information. Users will have access to information about these policies and procedures and the information will be easy to understand.

Members will make reasonable efforts so that users are made aware of the existence and location of their policies. Such efforts may include posting policies online and making available information on how to access and correct personal information.

## **9. Providing user access to personal information**

When users request it, members will tell them what personal information the member has about the user, what it is being used for, and to whom it has been disclosed, and will give them access to their information.

In certain situations, however, members may not be able to give users access to all personal information they hold about the user, e.g.:

- if it might reveal personal information about another user or could threaten the life or security of another individual;
- if it might reveal confidential commercial information;
- if the information is protected by solicitor-client privilege;
- if the information was generated in the course of a formal dispute resolution process; or
- if the information was collected in relation to the breach of an agreement or a law.

Members will explain the reasons for denying access when users ask.

In providing an account of the use and disclosure of personal information, members should state the source of the personal information where reasonably possible. Members will provide a list of the third parties to which it may have disclosed the user's personal information when it is not possible to provide an actual list.

In responding to a user's request, members will provide personal information in an understandable form, within a reasonable time and at minimal or no cost to the user.

Users will be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Members will keep records of any unresolved challenges regarding a user's personal information. Members will ensure that all subsequent transmissions of personal information shall include any amended information or the existence of any unresolved challenges. Where appropriate, members will transmit to third parties having access to the personal information in question any amended information and the existence of any unresolved challenges.

## **10. Handling users' complaints and questions**

Users may challenge a member's compliance with its own privacy code.

Members will have policies and procedures to receive, investigate and respond to users' complaints and questions. Members will make their complaint escalation process known to their users.

Members will respond to all complaints and questions in a timely manner under the circumstances.

*\*\*\* End of Document \*\*\**