



MCAP

THE MCAP GROUP OF COMPANIES

PRIVACY CODE

TABLE OF CONTENTS

<i>MCAP'S PRIVACY PHILOSOPHY</i>	3
OUR CONTINUING COMMITMENT TO YOU	3
WE LIVE BY IT – EVERYDAY	3
WHAT IS PERSONAL INFORMATION?	3
WHAT IS IN THIS CODE	3
APPLICATION OF THIS CODE	4
MCAP'S RELATIONSHIP WITH OTHER INVESTOR / LENDERS	4
THE REASONABLE PERSON APPROACH	4
MCAP'S PRIVACY PRINCIPLES	5
WHAT INFORMATION DOES MCAP COLLECT?	6
WHY AND WHAT TYPE OF INFORMATION IS COLLECTED	6
DISCLOSURE OF PERSONAL INFORMATION OUTSIDE OF MCAP	7
Sharing your Personal Information	8
EXCEPTIONS TO THE "NO COLLECTION, USE OR DISCLOSURE WITHOUT CONSENT" RULES	8
Collection	8
Use	8
Disclosure	9
SAFEGUARDING OF PERSONAL INFORMATION	9
RETENTION OF YOUR PERSONAL INFORMATION	10
OPT OUT POLICY	10
HOW YOU CAN HELP US PROTECT YOUR PERSONAL INFORMATION	11
Keeping Your Personal Information Accurate	11
DO YOU HAVE QUESTIONS OR CONCERNS?	12
RESPONSIBILITIES	12
KEEPING THIS PRIVACY CODE CURRENT	13
<i>SCHEDULE 1</i>	14
4.1 Principle 1 -- Accountability	14
4.2 Principle 2 -- Identifying Purposes	14
4.3 Principle 3 -- Consent	15
4.4 Principle 4 -- Limiting Collection	17
4.5 Principle 5 -- Limiting Use, Disclosure, and Retention	17
4.6 Principle 6 -- Accuracy	18
4.7 Principle 7 -- Safeguards	18
4.8 Principle 8 -- Openness	19
4.9 Principle 9 -- Individual Access	19
4.10 Principle 10 -- Challenging Compliance	20

THE MCAP GROUP OF COMPANIES PRIVACY CODE

MCAP'S PRIVACY PHILOSOPHY

The MCAP Group of Companies is committed to fairly and lawfully collecting and maintaining accurate personal information and to protecting the confidentiality of all personal information that we collect, retain, use or disclose to others in the course of our business activities.

OUR CONTINUING COMMITMENT TO YOU

Protecting the privacy and confidentiality of personal information has always been fundamental to the way we do business at MCAP. We strive to meet or exceed all the privacy standards established by federal, provincial and industry authorities in all our dealings with past, current and prospective customers.

WE LIVE BY IT – EVERYDAY

As a condition of their continuing employment, every MCAP employee annually signs a declaration acknowledging their agreement to be bound by the MCAP Code of Business Conduct, which includes both references to MCAP policies, such as this Privacy Code, and a confidentiality section obligating them to maintain the confidentiality of information both during and after their employment with MCAP.

MCAP has appointed a Privacy Officer and has established a Complaints Procedure to ensure compliance with this Privacy Code.

WHAT IS PERSONAL INFORMATION?

Personal information is information that identifies you as an individual. It includes your name and address, age and gender, also your personal financial records, identification numbers including your social insurance number, personal health information, personal references, and employment records.

WHAT IS IN THIS CODE

This Privacy Code has been developed to meet the standards set out in Canada's *Personal Information Protection and Electronic Documents Act* ("PIPEDA") and similar provincial legislation. The Privacy Code describes the principles MCAP will use to protect the privacy of personal information we possess about our clients, including sole proprietors and individuals carrying on business in a partnership, and establishes ethical and fair information management practices with respect to personal information collected, used or disclosed by the MCAP Group of Companies. The Code informs customers, be they

borrowers, depositors or our investors, and our business associates, how personal information is handled within the MCAP Group of Companies.

APPLICATION OF THIS CODE

This Privacy Code applies to all MCAP directors, officers, and employees with respect to any personal information in the possession or control of any of the MCAP Group of Companies, including MCAP Commercial LP, its general partner, 4223667 Canada Inc., MCAP Financial Limited Partnership, its general partner, MCAP Financial Corporation, MCAP Real Estate Finance Group Limited Partnership, its general partner, MCAP Real Estate Finance Group Inc., C-Cap Commercial Limited Partnership, C-Cap Commercial Inc., MCAP Service Corporation, and MCAP Leasing Inc. Reference throughout this Code to “MCAP”, “the Group”, “we”, “our” and “us” includes all of the above entities.

This Privacy Code does not apply to information about business customers carrying on business as corporations, partnerships or in other forms of association. The confidentiality of information with respect to those entities is protected at MCAP by our adherence to the applicable laws, our contracts with our business customers, MCAP’s Code of Business Conduct and MCAP’s other internal policies. This Code does, however, apply to information about officers, staff or principals of corporate clients, such as those providing personal guarantees of corporate loans.

MCAP’S RELATIONSHIPS WITH OTHER INVESTORS / LENDERS

MCAP is in the business of providing various financial services to its customers. This includes originating, underwriting and funding mortgage loans or leases to borrowers, primarily with monies provided to MCAP from institutional lenders / investors, who contract for MCAP to provide those services and to administer, manage, and collect payments on those loans or leases on their behalf and to report to them on the status of those financial assets.

The vast majority of funding through MCAP actually comes from these other investors / lenders. Given our requirement to report to these beneficial owners of the loans, MCAP must be able to disclose to them various personal information relating to the loans. This is why our documentation, such as our applications and commitment letters, contain your acknowledgement and consent to so disclose. We do so based on that consent and in accordance with this Code.

THE REASONABLE PERSON APPROACH

PIPEDA is really about sound information management practices. It requires an ethical, common sense, “reasonable person” approach to requesting, validating and maintaining personal information as a part of our business activities. Confidentiality is a sensitive topic. Many Canadians have raised concerns about the privacy of their personal information. Within MCAP we strive to understand what customers, clients and investors deem to be reasonable and then apply the principles in this Code.

MCAP'S PRIVACY PRINCIPLES

MCAP endorses and has adopted the ten privacy principals set out in full in Schedule 1 of PIPEDA. These ten privacy principles summarized below, embody sound and prudent information management practices. These practices will provide the necessary assurances that personal information obtained and utilized by MCAP in the course of its business activities will be accurate, held in confidence and be retained in a secure environment.

The full text of the ten principals is attached as Schedule 1 to this Code.

Principle 1 Accountability

MCAP takes responsibility for protecting and maintaining personal information under its control and has appointed a Privacy Officer to ensure compliance with these principles and PIPEDA.

Principle 2 Identifying the Purposes for Collecting Personal Information

MCAP will identify and disclose the reasons for which personal information is collected and used by MCAP at or before the time the information is collected.

Principle 3 Consent

MCAP will obtain an individual's informed consent for the collection, use or disclosure of personal information by MCAP, except as otherwise required or permitted by law.

Principle 4 Limits to the Collection of Personal Information

MCAP will limit the amount and type of personal information collected to that, which is necessary for its intended purposes. Personal information will be collected by fair and lawful means.

Principle 5 Limits to the Use, Disclosure and Retention of Personal Information

MCAP will not use or disclose personal information for purposes other than those for which it was collected, except with the consent of the individual, or as required or permitted by law. Personal information will be retained only as long as it is necessary to fulfill those purposes.

Principle 6 Accuracy

To minimize the possibility of inappropriate information being considered in its decision-making processes, MCAP will keep personal information as accurate, complete, and up-to-date as necessary for its intended purposes.

Principle 7 Safety & Security

MCAP will maintain appropriate safeguards to protect personal information from loss or theft, unauthorized access, disclosure, copying, use or modification regardless of the format in which it is retained.

Principle 8 Openness

MCAP will inform its customers, clients and employees about its policies and procedures regarding the management of personal information. MCAP will ensure that these policies and procedures are easily understood and readily available.

Principle 9 Individual Access

Upon request, MCAP will inform an individual of the existence, use and disclosure of his or her personal information and will provide the individual access to that information to verify and or update its accuracy and completeness.

Principle 10 Handling Inquiries

An individual will be able to direct an issue or concern regarding compliance with the above principles, or MCAP's practices to MCAP's Privacy Officer or to other accountable employees.

WHAT INFORMATION DOES MCAP COLLECT?

MCAP collects only the information that is needed for or related to the business purpose or product being requested.

MCAP obtains personal information about you primarily from you. MCAP may also obtain additional information from other sources with your consent. For example, when you apply for a mortgage, MCAP asks you to authorize us to obtain a credit bureau report on you (if you have not already so authorized your mortgage broker), and to collect and verify your personal information with the credit bureau, credit insurers, your employer, personal references, and other lenders. If you do not authorize us to obtain your credit bureau report, and to verify your personal information, our standard lending practices may not allow us to provide you with a positive response to your mortgage request. When you are applying for other products or services, such as a debenture, MCAP will also ask you for your social insurance number so we can report, for taxation purposes, interest earned.

WHY AND WHAT TYPE OF INFORMATION IS COLLECTED

MCAP wants to work with you to help you achieve your goals, to provide you with value-added service on an ongoing basis, and to establish a lasting relationship with you as your needs grow and change. The better MCAP knows you, the better we are able to serve you. MCAP therefore asks you for your personal information for the following purposes:

- to identify you, thereby protecting us both from error and fraud;
- to understand your needs;
- to determine the suitability of our products and services for you;
- to determine your eligibility for our products and services;
- to provide you with information and offers on our products and services, or those of our business associates, that MCAP believes may be of interest to you, and
- to comply with applicable laws.

There are some purposes, which are self-evident. For example, if you are applying for a mortgage, MCAP asks for information concerning your credit history and for personal references, which MCAP may use to verify the information you provided and to underwrite your loan application. MCAP may also obtain information about you from other sources in order to better understand and meet your needs and goals.

In general, you can choose not to provide us with some or all of your personal information. However, you must understand that if you make this choice, MCAP may not be able to provide you with the product, service, or information that you requested or that was or could be offered to you.

MCAP will make sure you are aware of the purposes for collecting information when you apply for any of our products or services. Self-evident purposes should be clear, but if you have any questions, just ask us. If a new purpose for using your personal information develops, MCAP will ask for your consent again.

DISCLOSURE OF PERSONAL INFORMATION OUTSIDE OF MCAP

MCAP has a strict policy of not releasing personal information about our customers, subject to the important exceptions discussed below.

The most common reason for release of your personal information is that you have given your consent. For example, when you apply for a mortgage and accept our commitment letter, you give your consent to the exchange of information about you with a credit bureau, other credit grantors, credit insurers including mortgage and portfolio insurers and other lenders who invest in or fund our mortgage and lease financing products.

Other reasons may include if we have a legal obligation, such as a court order, or if we need to protect assets (e.g. collection of overdue accounts) or the public's interest. For example, we may release personal information about a customer to legal authorities in cases of criminal activity, or for the detection and prevention of fraud. If we release information for any of these reasons, we keep a record of what, when, why and to whom such information was released.

We do not keep a record of why your personal information is disclosed to third parties for routine purposes such as reporting to Canada Customs and Revenue Agency (T5 and other reports), regular update reports to a credit bureau, credit insurers and investors / lenders, and reporting to third parties when cheques are returned NSF (i.e. for insufficient funds).

Any health information that you may provide for credit insurance purposes (i.e. mortgage life insurance) is forwarded only to the insurer in question and is not used by us for any other purpose.

MCAP does not sell lists of our customers to others for their use, although institutional investors who have funded your loan and for whom MCAP provides mortgage administration services are entitled, as per your consent in our commitment letters, to receive your personal information.

SHARING YOUR PERSONAL INFORMATION

Your personal information is shared, to the extent permitted by law, and to the extent necessary to provide you with the best service, within the MCAP Group of Companies and our institutional business affiliates in order to provide mortgages, debentures, insurance and other products and services. This sharing is limited to a “need to know” basis. With our various departments having a more comprehensive understanding of your requirements, we are better able to meet your needs as they grow and change.

MCAP routinely collects and collates anonymous, non-personal information that is not traced back to a specific individual or business client. This includes individual and cumulative transaction and settlement records with our various investors. This type of information is considered necessary and consistent with the MCAP business activity.

EXCEPTIONS TO THE “NO COLLECTION, USE OR DISCLOSURE WITHOUT CONSENT” RULES

The limited exceptions, applicable to MCAP, relating to obtaining consent for the collection, use or disclosures of personal information include the following:

COLLECTION

MCAP is authorized by PIPEDA to collect personal information without the knowledge or consent of the individual where:

1. collection of the personal information is clearly in the interests of the individual and consent cannot be obtained in a timely manner;
2. it is reasonable to expect that collection of the personal information with the knowledge or consent of the individual would compromise the availability or accuracy of the information and the collection is reasonable for purposes of investigating a breach of an agreement or contravention of federal or provincial law; or
3. the information is publicly available and is specified by regulations issued by federal legislation.

USE

MCAP is authorized by PIPEDA to use personal information, without the knowledge or consent of the individual, in circumstances including where:

1. the personal information was originally collected without consent, express or implied, and collection was clearly in the interests of the individual and consent could not be obtained in a timely manner;
2. the information was originally collected without consent, express or implied, in circumstances where collection with the knowledge and consent of the individual would compromise the availability or accuracy of the information and the collection was reasonable for the purposes of investigating a breach of an agreement or a contravention of federal or provincial law;
3. MCAP has reasonable grounds to believe the information could be useful in the investigation of a contravention of federal, provincial or foreign law, that has been, is being, or is about to be committed, and the information is used for the purpose of investigating that contravention;
4. it is used with respect to an emergency that threatens the life, health or security of an individual;
5. it is used for statistical, or scholarly study or research purposes, under limited conditions approved by the Privacy Commissioner; and/or
6. the information is publicly available and is specified by the Regulations to PIPEDA.

DISCLOSURE

PIPEDA authorizes MCAP to disclose personal information without the knowledge or consent of the individual in circumstances including if such disclosure:

1. is made, within the Province of Quebec, to an advocate or notary or, in any other province, a barrister or solicitor who is representing MCAP;
2. is for the purpose of collecting a debt owed by the individual to MCAP;
3. is required to comply with a subpoena or warrant issued, or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;
4. is made to a government institute that has identified its lawful authority to obtain the information, and which has indicated (i) it suspects the information relates to national security, the defense of Canada, or the conduct of international affairs, or (ii) disclosure is requested for the enforcement of federal, provincial or foreign law, carrying out an investigation relating to such enforcement, or gathering intelligence for the purpose of such enforcement, or (iii) disclosure is requested for the purpose of administering a federal or provincial law;
5. is made to an investigative body or government institution on the initiative of MCAP, and relates to a breach of an agreement or a contravention of federal, provincial or foreign law; or where MCAP suspects the information relates to national security, the defense of Canada or the conduct of international affairs;
6. is made because of an emergency that threatens the life, health or security of an individual and MCAP informs the individual without delay of the disclosure; and/or
7. is made for statistical or scholarly study and research purposes, under limited conditions, approved by the Privacy Commissioner.

SAFEGUARDING OF PERSONAL INFORMATION

Your personal information is secure within MCAP. We have comprehensive security controls to protect against unauthorized use, alteration, duplication, destruction, disclosure, loss or theft of, or unauthorized access to, your personal information.

MCAP may use other companies to provide services to you on our behalf, such as the printing of correspondence, storage of your files in a secured environment or to conduct customer satisfaction surveys on our behalf. In such cases, we will have contracts in place holding these companies to the same high standards of confidentiality by which we are governed and requiring that any information provided by us must be kept strictly confidential and used only for the purposes of the contract.

MCAP also has agreements in place with credit insurers and other institutional investors / lenders, which also require that any information provided by us must be maintained in strict confidence.

MCAP ensures the physical, organizational and electronic security of your personal information through the use of secure locks on filing cabinets and doors, and restricted access to our information processing and storage areas. MCAP limits access to relevant information to authorized employees only, and through the use of pass keys and computer passwords and, where necessary, the encryption of electronically transmitted information.

MCAP has procedures in place when destroying, deleting or disposing of personal information when it is no longer required for the purposes as set out in this Code, or by law, to prevent unauthorized access to such personal information.

RETENTION OF YOUR PERSONAL INFORMATION

MCAP only keeps your personal information for as long as we need it to meet the purposes set out in this Code. The length of time we retain your personal information is also affected by: (1) the type of product or service you have from us, and (2) any legal requirements we may have to meet such as regulatory file retention periods or for being able to respond to any concerns you may have even if you are no longer a customer of ours.

OPT OUT POLICY

You can choose not to provide us with some or all of your personal information. This may, however, severely restrict the products and services MCAP can then provide. You can also withdraw your consent to our use of your personal information, as long as you give us notice in writing, addressed to:

Single Family

“MCAP Privacy Information”
c/o MCAP Service Corporation
200 – 101 Frederick Street
Kitchener, ON N2G 3Y9

Leasing

“MCAP Privacy Information”
c/o MCAP Leasing Inc.
5575-300 North Service Road
Burlington, ON L7L 6M1

- withdrawing your consent does not result in our or your inability to fulfill your financial (mortgage / debenture / lease) contract already in place with us; and
- your consent does not relate to a credit product we have granted to you, where we are required to collect and exchange some or all of your personal information on an ongoing basis, with credit insurers, other investors / lenders, or a credit bureau or to maintain the integrity of the credit-granting system and the completeness of information held by a credit bureau.

HOW YOU CAN HELP US PROTECT YOUR PERSONAL INFORMATION

If you want to review or verify your personal information, or find out to whom we have disclosed it as permitted by this Code, you can call and speak to one of our service representatives at our Call Centre. At that time, if it is not something that can be simply answered over the phone, we will provide you with a form to sign and will help you complete the specific information we will need from you to enable us to search for, and provide you with, the requested personal information we hold about you. We may charge you a fee to do this and will advise you of the fee in advance.

There are a few instances where we will not be able to provide the personal information we hold about you that you request. Some of these instances include, if:

- it contains references to other persons;
- it is subject to solicitor-client or litigation privilege;
- it contains our own proprietary information that is confidential to us;
- it has already been destroyed due to legal requirements or because we no longer needed it for the purposes set out in this Code;
- it is too costly, in our determination, to retrieve;
- we are prohibited by law from disclosing to you.

If we are unable to provide you with access to your personal information, we will explain the reason why.

Remember that in most provinces you have the right to access and verify the personal information held about you by a credit bureau. To do so, you must speak directly to the appropriate bureau.

KEEPING YOUR PERSONAL INFORMATION ACCURATE

We are committed to maintaining the accuracy of your personal information for as long as it is being used for the purposes set out in this Code. You play an active role in keeping us up-to-date. Prompt notification of any changes, for example to your address or telephone number, will help us provide you with the best possible service. Should you discover, upon review of your personal information, that amendments are required, please advise us.

If we do not agree to make the amendments that you request, you may challenge our decision. We will make a record of this challenge, which will be kept on file.

DO YOU HAVE QUESTIONS OR CONCERNS?

If you have privacy questions, concerns or complaints, we want them to be answered satisfactorily or resolved as quickly as possible and ask that you follow, in order, the following three steps.

First: Contact the person at MCAP you have been dealing with or call our Customer Service Centre and speak to a representative. They can usually handle most questions or concerns immediately over the phone.

Second: If the Customer Service Representative or the employee you dealt with is unable to resolve the matter to your satisfaction, advise them that you wish the matter to be reviewed by the department manager who will contact you to resolve the issue. You may be asked to put your concern or complaint in writing.

Third: If you are still not satisfied contact MCAP's Privacy Officer at:

MCAP Privacy Officer
Suite # 400
200 King Street West
Toronto, ON M5H 3T4
(416) 598-2665

Upon completion of review by MCAP's Privacy Officer, if the above steps fail to resolve your concern to your satisfaction, your issue may be reviewed by the Privacy Commissioner of Canada who you may contact at any time in this process, by writing to:

The Privacy Commissioner of Canada
112 Kent Street
Ottawa, ON K1A 0H2

or

by telephone, toll free, at 1-800-282-1376
by facsimile at 613-947-6850

RESPONSIBILITIES

Any MCAP employee who believes personal information is not being handled in accordance with this Policy should immediately so advise their manager and the Privacy Officer.

Department Managers required to resolve privacy issues (as per the second step in our privacy question and complaint handling process) shall maintain appropriate records of the same and shall report them to the Privacy Officer.

Department Managers are responsible for oversight of this Policy within their department, including establishing, implementing and regularly reviewing the necessary procedures and standards to give effect to this Policy and to train their staff accordingly.

MCAP's General Counsel & Corporate Secretary is responsible for providing advice and assistance to the Privacy Officer and the Department Managers on appropriate compliance programs and for reviewing the effectiveness of such programs.

The Privacy Officer shall act as a resource to Department Managers in the handling of disputes and shall present a summary report annually to the Compliance and Governance Committee of the Board of 4223667 Canada Inc. with respect to unresolved privacy disputes, the nature and number of privacy issues reviewed and any recommendations with respect to privacy strategies, oversight and policies.

The Privacy Officer will assist Department Managers with developing procedures, standards, guidelines and interpretations, promoting awareness of privacy issues and developing staff training programs.

KEEPING THIS PRIVACY CODE CURRENT

Changes to this Privacy Code and the information handling practices of MCAP will result in amendments to this document from time to time. The Code will be reviewed by the Privacy Officer at a minimum, annually. MCAP may add, delete or modify sections at its discretion. The date of the current version can be found on the cover page.

SCHEDULE 1

(Section 5)

PRINCIPLES SET OUT IN THE NATIONAL STANDARD OF CANADA ENTITLED *MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION, CAN/CSA-Q830-96*

4.1 Principle 1 -- Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

4.1.1

Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

4.1.2

The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.

4.1.3

An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

4.1.4

Organizations shall implement policies and practices to give effect to the principles, including

- (a)* implementing procedures to protect personal information;
- (b)* establishing procedures to receive and respond to complaints and inquiries;
- (c)* training staff and communicating to staff information about the organization's policies and practices; and
- (d)* developing information to explain the organization's policies and procedures.

4.2 Principle 2 -- Identifying Purposes

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

4.2.1

The organization shall document the purposes for which personal information is collected in order to comply with the Openness principle (Clause 4.8) and the Individual Access principle (Clause 4.9).

4.2.2

Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfil these purposes. The Limiting Collection principle (Clause 4.4) requires an organization to collect only that information necessary for the purposes that have been identified.

4.2.3

The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

4.2.4

When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to the Consent principle (Clause 4.3).

4.2.5

Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

4.2.6

This principle is linked closely to the Limiting Collection principle (Clause 4.4) and the Limiting Use, Disclosure, and Retention principle (Clause 4.5).

4.3 Principle 3 -- Consent

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

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 the individual 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.

4.3.1

Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

4.3.2

The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

4.3.3

An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.

4.3.4

The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

4.3.5

In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

4.3.6

The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

4.3.7

Individuals can give consent in many ways. For example:

- (a) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;
- (b) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;
- (c) consent may be given orally when information is collected over the telephone; or
- (d) consent may be given at the time that individuals use a product or service.

4.3.8

An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.

4.4 Principle 4 -- Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

4.4.1

Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Clause 4.8).

4.4.2

The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

4.4.3

This principle is linked closely to the Identifying Purposes principle (Clause 4.2) and the Consent principle (Clause 4.3).

4.5 Principle 5 -- Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

4.5.1

Organizations using personal information for a new purpose shall document this purpose (see Clause 4.2.1).

4.5.2

Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.

4.5.3

Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

4.5.4

This principle is closely linked to the Consent principle (Clause 4.3), the Identifying Purposes principle (Clause 4.2), and the Individual Access principle (Clause 4.9).

4.6 Principle 6 -- Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

4.6.1

The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

4.6.2

An organization shall not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected.

4.6.3

Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

4.7 Principle 7 -- Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

4.7.1

The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

4.7.2

The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.

4.7.3

The methods of protection should include

- (a) physical measures, for example, locked filing cabinets and restricted access to offices;
- (b) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and
- (c) technological measures, for example, the use of passwords and encryption.

4.7.4

Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

4.7.5

Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).

4.8 Principle 8 -- Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

4.8.1

Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

4.8.2

The information made available shall include

- (a) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;
- (b) the means of gaining access to personal information held by the organization;
- (c) a description of the type of personal information held by the organization, including a general account of its use;
- (d) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and
- (e) what personal information is made available to related organizations (e.g., subsidiaries).

4.8.3

An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.

4.9 Principle 9 -- Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Note: In certain situations, an organization may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request. 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, and information that is subject to solicitor-client or litigation privilege.

4.9.1

Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical

practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

4.9.2

An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.

4.9.3

In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual.

4.9.4

An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.

4.9.5

When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

4.9.6

When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.

4.10 Principle 10 -- Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

4.10.1

The individual accountable for an organization's compliance is discussed in Clause 4.1.1.

4.10.2

Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.

4.10.3

Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist. For example, some regulatory

bodies accept complaints about the personal-information handling practices of the companies they regulate.

4.10.4

An organization shall investigate all complaints. If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.