

Guidelines for Developing a Personal Information Code for Professional Regulatory Organizations

Revised April 2005

Produced by:

Access and Privacy Branch
Alberta Government Services
3rd Floor, Commerce Place
10155 – 102 Street
Edmonton, AB T5J 4L4
Phone: (780) 644-7472
Toll free dial 310-0000 first
Fax: (780) 427-1120
Web site: www.pipa.gov.ab.ca

Published October 2003

Revised April 2005

ISBN 0-7785-3683-1

Note: The *Personal Information Protection Act* came into force on January 1, 2004. These guidelines are an administrative tool intended to assist professional regulatory organizations that wish to develop a personal information code. It is not intended as, nor is it a substitute for, legal advice. For the exact wording and interpretation of PIPA, please read the Act and its regulation in their entirety.

Guidelines for Developing a Personal Information Code for Professional Regulatory Organizations

CONTENTS

I. INTRODUCTION	1
PIPA and Professional Regulatory Organizations.....	1
Advantages and Disadvantages of Developing a Personal Information Code.....	2
Process for Developing, Approving and Reviewing a Code.....	3
II. SAMPLE ARTICLES	7
1 Definitions.....	7
2 Scope and Application.....	9
3 Privacy Principles	10
3.1 Accountability.....	10
3.2 Consenting to the Collection, Use and Disclosure of Personal Information ...	11
3.3 Collecting Personal Information	12
3.4 Using Personal Information.....	14
3.5 Disclosing Personal Information	14
3.6 Collecting, Using and Disclosing Personal Employee Information.....	15
3.7 Giving Access to and Correcting Personal Information.....	16
3.8 Accuracy	19
3.9 Protection.....	20
3.10 Retention	20
4 Procedure For Handling Complaints	21
5 Monitoring/Reviewing the Operation of the Code.....	22
6 Establishing the Code	23
7 Publication of the Code	23

I. INTRODUCTION

PIPA and Professional Regulatory Organizations

The *Personal Information Protection Act* (PIPA or the Act) establishes a framework for a consistent set of privacy principles and standards for the private sector. The fair information principles in the Act set out the minimum requirements for how private sector organizations can collect, use, disclose and protect personal information. In addition, the Act gives individuals a right to know what information an organization holds about them and a right to ask for it to be corrected if it is wrong. The Act also allows individuals to complain to the Information and Privacy Commissioner of Alberta (the Commissioner) about the way their personal information is being handled by organizations or about decisions on their access or correction requests.

Professional regulatory organizations (PROs) under the Act are generally self-governing professional or occupational bodies, incorporated under an Act that provides for the regulation of that profession or occupation. These bodies regulate the standards of education and experience required of members to enter the profession or occupation, their standards of practice, continuing education requirements and conduct of members, and investigate and adjudicate complaints from the public or other members about alleged unprofessional conduct. Examples of PROs include the Law Society of Alberta, the Institute of Chartered Accountants of Alberta, and the Association of Professional Engineers, Geologists and Geophysicists of Alberta.

Part 6, section 55, of the *Personal Information Protection Act* and Part 7 of the PIPA Regulation contain special provisions that enable professional regulatory organizations to balance the protection of personal information with their mandate to protect the public interest.

These provisions allow PROs to develop personal information codes that provide the same level of privacy protection as the Act while allowing some latitude in format and wording. A “personal information code” means a code governing the collection, use and disclosure of personal information in a manner that is consistent with the purposes and intent of sections 1 to 35 of PIPA and related provisions of the PIPA Regulation. A PRO has the option of directly following sections 1 to 35 of PIPA and provisions of the PIPA Regulation dealing with privacy protection or deciding that its membership and the public would be better served by having a tailored personal information code. Such a code would allow a PRO to address its unique concerns and outline its privacy protection measures using profession-specific wording and format. However, Parts 4 and 5 of the Act (the Commissioner’s process and powers for investigating complaints and conducting reviews) will still apply to a PRO that has a personal information code.

For PROs that decide to establish their own personal information codes, these *Guidelines for Developing a Personal Information Code* are intended to provide sample provisions and commentary to assist in the development process.

Advantages and Disadvantages of Developing a Personal Information Code

Advantages

A personal information code:

- May serve to put the privacy principles of PIPA into context for the particular profession or occupation;
- May give the PRO a sense of ownership of its privacy obligations and put it in an active position rather than just being a passive recipient of legislative obligations;
- May send a positive statement to the public that the PRO is responsive to the privacy concerns of individuals and is active in protecting their privacy rights (e.g. by adopting a code that meets or exceeds the standard for privacy protection required by PIPA or by using independent audits or monitoring programs to reinforce the organization's commitment to transparency and accountability);
- May enable a PRO to develop a code in a manner that allows it to harmonize the code with other elements of its governing legislation as well as bylaws and rules of conduct;
- May help change the culture of a PRO by raising the awareness of privacy and by introducing a compliance regime;
- May enable a PRO to use an existing internal complaint-handling or dispute resolution process for individuals seeking redress (although such a process does not prevent an individual from making a complaint to the Information and Privacy Commissioner under the Act);
- May enable a PRO to develop a simplified version of the principles set out in the Act that would be directly relevant and meaningful to the profession, its members and the public.

Disadvantages

A personal information code:

- May provide less certainty for members and the public than following the provisions in the Act, at least until the code provisions are interpreted by the Information and Privacy Commissioner;
- Must be developed, implemented and kept up-to-date; developing and administering the code requires a PRO to have sufficient resources to carry out this function;

- May not be necessary or advantageous if the PRO can prepare its own explanatory material or policies on the application of the Act in the context of the particular profession or occupation;
- May not be appropriate if the PRO does not need to promote cultural change through the introduction of a privacy code.

Process for Developing, Approving and Reviewing a Code

Draft a code to a professional standard using language that is clear and easy to understand.

- A personal information code will replace all or some of sections 1 to 35 of PIPA and will be binding upon the members of the particular profession or occupation as though it were a piece of legislation. It is therefore important that a code be carefully drafted to an appropriate legal standard, especially if it contains a complaint-handling mechanism.
- A personal information code must not be established in a regulation or in a bylaw, rule of conduct, or policy of the PRO. It should be a free-standing document.
- It should be written to a professional standard using language that is clear, unambiguous and makes it easy for individuals to understand their rights and obligations.
- Try not to use professional jargon that some individuals may not fully understand and, if the code uses profession-specific language, include a list of definitions to explain the terms.
- Each paragraph should be numbered or lettered to help with communication, application and compliance.
- If the code includes a complaint or review procedure, it should clearly specify that an individual is not precluded from making a complaint to or requesting a review by the Commissioner (under Parts 4 and 5 of PIPA), regarding a matter addressed by the code.
- If the PRO does not have expertise in drafting codes, it may be useful to obtain outside help from legal and plain language experts.

Consult with members of the PRO on drafts of the code.

- The PRO should consult with its members on drafts of the code. It should use a consultation process similar to what it would use to consult with members on draft new or amended regulations such as standards of practice or similar instruments.

- As a best practice, the PRO may wish to consult with relevant stakeholders, including members of the public, on drafts of the code to ensure that the code adequately meets the needs and expectations of those stakeholders and the public. The credibility and integrity of a code depends in part on it gaining support and acceptance from both stakeholders and members of the public.

Ensure that the provisions of the code are consistent with the purpose and intent of sections 1 to 35 of the Act.

- The Act requires that a personal information code be consistent with the purposes and intent of sections 1 to 35 of the Act and with any of the regulations under PIPA that deal with privacy protection.
- A personal information code must indicate which provisions of sections 1 to 35 that it intends to replace or indicate that it intends to replace all of those sections. It should also clearly indicate whether the code will apply to all personal information collected, used or disclosed by the PRO or just to certain categories of personal information in the custody or under the control of the PRO. For example, will the code only apply to registered members of the PRO or will it also apply to employees of the PRO or to individuals named in disciplinary investigations?
- If an obligation under a personal information code differs from an obligation under the Act, the organization should say, in commentary under the relevant article of the code, what the rationale for the difference is and how, in the opinion of the PRO, the obligations in the code are at least consistent with the purposes and intent of sections 1 to 35 of the Act and the Regulation.
- A PRO may include profession-specific language in order to customize the privacy principles for that profession.
- A PRO may add to the Act's requirements by including higher standards in a policy statement that could follow the related privacy article in the code. For example, a policy of the PRO may require an individual to consent to the use or disclosure of his or her personal information even where the Act allows for this without consent.

Have the code approved by the governing council or governing body of the professional regulatory organization.

- A code should be approved by the governing council or body of a PRO. The PRO should adopt whatever process it would normally use for the approval of a code that is binding on all its members.
- The code must specify the way in which the PRO approves or otherwise establishes the code.

Promote the code and make it available on request.

- A PRO must make a copy of the code and any relevant explanatory material available to any person on request.
- If a code includes a complaint-handling procedure, the PRO should promote the code more widely in the media or on its web site.
- The PRO must state in the code how it will publish the code in printed or electronic form.

Commit sufficient resources to administer the code.

- The code should include a commitment to provide sufficient resources to ensure its proper administration.

Include a process for review of the code.

- A code must include a process for reviewing its operation at regular intervals (e.g. every 3 years). The review process could be similar to the process that enabled the code to be approved by the governing body of the PRO.
- A PRO must allocate sufficient resources to the review of the code.
- The PRO may wish to have a requirement in policy that a copy of the report of the review be sent to the Office of the Information and Privacy Commissioner.

Request an order from the Minister responsible for PIPA.

- Once a PRO has developed its code and had it approved by its governing body, it may request that the Minister responsible for PIPA grant an authorization that the PRO's personal information code will operate in the place of the sections of the Act and Regulation that are addressed in that code.
- The written request must include a proposed coming-into-force date for the code and must be signed by a person authorized to sign on behalf of the governing body of the PRO. A copy of the code must also be included with the request.
- The Minister may grant an authorization and direct that the PRO's personal information code will operate in the place of the sections of the Act and Regulation that are addressed in the code. The Minister may impose any terms and conditions that the Minister considers appropriate.
- If a PRO makes a material change to its code, it must resubmit the code to the Minister. The Minister may revoke the authorization for the old code and grant an authorization for the new code, directing that the new code will operate in the place of the sections of the Act and Regulation that are addressed in the new code.

II. SAMPLE ARTICLES

PERSONAL INFORMATION CODE FOR THE [NAME OF PROFESSIONAL REGULATORY ORGANIZATION]

Because this is a sample code, the articles are often followed by commentary, alternatives or examples. This additional information is placed in either square brackets or boxes following the relevant article.

The format followed for the sample code below is only presented as a suggestion. A professional regulatory organization (PRO) may prefer to set out each article of the code followed by statements of policy that are clearly indicated as such.

1 Definitions

Act means the *Personal Information Protection Act*.

Business contact information means an individual's name, position name or title, business telephone number, business address, business e-mail, business fax number and other similar business information collected, used or disclosed to contact an individual in his or her capacity as an employee or official of an organization.

Code means a personal information code (see definition below).

Collection means gathering, acquiring, recording, photographing or obtaining personal information from any source, and by any means.

Commissioner means the Information and Privacy Commissioner appointed under the *Freedom of Information and Protection of Privacy Act*.

Complainant means an individual who lodges a complaint with the professional regulatory organization or with the Commissioner.

Disclosure means showing, telling, sending, or giving personal information to some other individual or organization or the public, but does not include use of the information within the professional regulatory organization.

Employee means an individual employed by the professional regulatory organization and includes an individual who performs a service for or in relation to or in connection with the professional regulatory organization as an apprentice, volunteer, participant or student, or under a contract or an agency relationship with the professional regulatory organization.

Investigation means an investigation related to a breach of agreement, a contravention of an enactment of Alberta or Canada or of another province of Canada, or circumstances or conduct that may result in a remedy or relief being available at law, if the breach,

contravention, circumstances or conduct in question has or may have occurred or is likely to occur and it is reasonable to conduct an investigation.

Member means a member of a professional regulatory organization.

Minister means the Minister determined under section 16 of the *Government Organization Act* as the Minister responsible for the *Personal Information Protection Act* (currently the Minister of Government Services).

Personal employee information means, in respect of an individual who is an employee or a potential employee, personal information reasonably required by the professional regulatory organization that is collected, used or disclosed solely for the purposes of establishing, managing or terminating an employment relationship or a volunteer work relationship between that individual and the professional regulatory organization, but does not include personal information about the individual that is unrelated to that relationship.

Personal information means information about an identifiable individual.

Personal information code means a code governing the collection, use and disclosure of personal information by a professional regulatory organization in a manner that is consistent with the purposes and intent of sections 1 to 35 of PIPA.

PIPA means the *Personal Information Protection Act*.

PIPA Regulation means the regulation enacted under the *Personal Information Protection Act* (AR 366/2003).

Professional Act means an enactment under which a professional or occupational group or discipline is organized and that provides for the membership in and the regulation of the members of the professional or occupational group or discipline including such matters as registration, competence, conduct, practice and discipline of its members.

Professional regulatory organization means an organization incorporated under a professional Act.

Public body means a public body as defined in the *Freedom of Information and Protection of Privacy Act*.

Use means employing personal information to carry out purposes identified by the professional regulatory organization or other purposes permitted by the Code.

The Code should include a section defining key terms used in the Code. These may include some of the above terms as well as other terms the PRO considers relevant.

2 Scope and Application

- 2.1 This Code applies to all personal information of members and employees of the _____ [name of professional regulatory organization] and of members of the public who may contact the _____ [name of PRO] or lodge a complaint with the _____ [name of PRO] that is in its custody or under its control.

Alternatively, the Code could be made to apply only to the personal information of regulated members but not to that of employees or members of the public, or it could be made to apply to activities dealing with the registration and regulation of members, including investigation of complaints and other disciplinary matters, but not to any other administrative matters of the PRO.

- 2.2 This Code does not apply to the personal information of _____.

This is only needed if the PRO is going to exclude certain categories of personal information from the coverage of the Code. It is important to clearly set out any categories of personal information to which the Code does not apply. Otherwise, members, employees and the public will assume that it is intended to apply to all personal information in the custody or under the control of the PRO.

- 2.3 This Code replaces sections _____ of the *Personal Information Protection Act* (PIPA) and sections _____ of the PIPA Regulation as they apply to privacy protection for the personal information of the individuals in [Article 2.1](#).

The PRO will fill in the relevant section numbers of PIPA and the PIPA Regulation that the Code is replacing. The Code might address all of sections 1-35 of the Act or it might only address certain sections, such as those dealing with consent, collection, use, disclosure, protection, accuracy and retention, but not with respect to the process for handling access and correction requests.

It is very important that the PRO clearly states in its Code what is not covered by the Code.

3 Privacy Principles

3.1 Accountability

- 3.1.1 The _____ [name of governing body or council of the PRO] is responsible for all personal information set out in [Article 2.1](#) that is either in our custody (i.e. possession) or under our control.

Custody and control can be explained in greater detail. For example, “personal information that is in our offices, file cabinets, computers, etc. and that is in the custody of our contractors, volunteers, students or agents.”

- 3.1.2 The _____ [name of governing body or council of the PRO] will designate (appoint) one or more persons within the _____ [name of PRO] to be responsible for ensuring that we comply with this Code. Other individuals may be delegated to act on behalf of the designated person(s).

- 3.1.3 We will publish the title and contact information of the person(s) designated to oversee compliance with this Code.

The PRO could specify in the Code or in its policy where it will publish this information, for example, on its web site or in a brochure.

- 3.1.4 We will develop and follow policies and practices that are reasonable for us to meet our obligations under this Code and make information about these policies and practices available to any person on request.

Alternatively, a PRO could say that this information will be published on its web site. A PRO could also refer to the presence of any policies and/procedures that may be found in a separate document.

- 3.1.5 We will ensure that there are sufficient resources allocated to administer this Code.

- 3.1.6 In carrying out our responsibilities under this Code, we will do what a reasonable person would think was appropriate in the circumstances.

3.2 Consenting to the Collection, Use and Disclosure of Personal Information

3.2.1 Before we collect, use or disclose personal information, we will ask the individual that the information is about to consent to the collection, use and disclosure of the personal information or to consent to the collection of the personal information from someone who is not the individual, unless this Code says otherwise.

3.2.2 We do not need to obtain consent to collect, use or disclose personal information in the specific circumstances set out in [Article 3.3.5](#) (collection without consent), [Article 3.4.2](#) (use without consent), [Article 3.5.2](#) (disclosure without consent) and Articles [3.6.1](#) and [3.6.3](#) (personal employee information).

Do not include a reference to Articles [3.6.1](#) and [3.6.3](#) if it is not intended that the Code apply to employees of the PRO.

3.2.3 We will not require an individual to consent to the collection, use or disclosure of personal information as a condition of providing a service to the individual unless the collection, use or disclosure is required to carry out a purpose identified in [Article 3.3.2](#).

3.2.4 When an individual applies for registration with the _____ [name of PRO], this constitutes implied consent for us to collect, use and disclose the individual's personal information for purposes related to the registration of the individual as a member of _____ [name of PRO].

3.2.5 We will only use opt-out consent if we tell individuals what the purposes are for collecting, using or disclosing their personal information, we notify them at the time of the collection, use or disclosure that they have the option to opt-out, we give them a reasonable chance to say no to the collection, use or disclosure, and the information in question is not considered sensitive.

This clause may be added to a Code if a PRO intends to use opt-out consent.

3.2.6 An individual may change or withdraw his or her consent by giving us reasonable notice of this as long as this would not change or frustrate a legal obligation between the individual and us. When we receive such a notice, we will inform the individual of the likely consequences (if any) of changing or withdrawing his or her consent.

3.2.7 We will obtain consent to the collection, use or disclosure of personal information without giving false or misleading information about the collection, use or disclosure or using deceptive or misleading practices.

A PRO may wish to add the following policy statements:

Policy statements:

We will use consent clauses that are easy to find, clearly worded and as specific as possible regarding the purposes of collection, use or disclosure.

We will obtain express consent wherever possible. In determining what form of consent to use, we will take into account the sensitivity of the personal information and the reasonable expectations of our members (and our employees and the public).

We may obtain consent in person, by telephone, by mail or Facsimile or via the Internet (e-mail).

Note: A PRO must establish procedures for authenticating the identity of the individual giving consent. A PRO must use a format that will allow for a record of the consent to be produced on paper, if requested. If consent is given by electronic means, a PRO must comply with the *Electronic Transactions Act*.

3.3 Collecting Personal Information

3.3.1 We will only collect personal information for purposes that are reasonable and we will only collect the information that is reasonable for carrying out those purposes.

3.3.2 We will collect personal information only for the following purposes (referred to in this Code as “identified purposes”):

A PRO should review its own professional statute, regulations, bylaws and rules to determine what personal information it collects and for what purposes and include those purposes here. Some examples of purposes follow by way of illustration only:

- creating and maintaining records about applications for and obtaining registration as a member;
- creating and maintaining records about applications for and obtaining a practice permit and for keeping records about suspended, cancelled or reinstated practice permits;
- creating and maintaining records about members fulfilling their continuing education or continuing competence requirements;
- lodging, investigating and conducting hearings and appeals concerning complaints against members;
- meeting other legal and regulatory requirements.

- 3.3.3 We will notify our members, prospective members or members of the public about the identified purposes before or at the time the personal information is collected and we will do this orally, electronically or in writing. We will also let them know who they can contact if they have questions about the collection of their personal information.

The collection, use and disclosure of personal information of employees is dealt with separately in Articles [3.6.1](#) to [3.6.4](#).

- 3.3.4 We will only collect personal information directly from the individual the information is about unless the individual consents to the collection of information from another source or the information may be collected without consent under [Article 3.3.5](#).

- 3.3.5 We may collect personal information without consent of the individual only in the following specified circumstances:

- when a reasonable person would consider that it is clearly in the interests of the individual and we cannot obtain consent in a timely way or the individual would not reasonably be expected to withhold consent;

For example, collecting information from a member about his or her spouse who is a named beneficiary for a certain member benefit program.

- when another Act or regulation requires or allows for collection without consent;

Provide some examples of commonly used Acts or regulations that allow the PRO to collect personal information without consent, e.g. _____ *Profession Act* [indicate the section(s)], the *Employment Insurance Act*, the *Income Tax Act*.

- if the collection is reasonable for the purposes of an investigation or legal proceeding;
- if we are determining whether an individual is suitable for an honour, award or other similar benefit;
- if the information is needed to collect a debt owing to us or for us to repay money owing to the individual;
- if the information is publicly available as defined in the PIPA Regulation;

- if the information can be disclosed to us without consent by a public body or organization; or
- if the collection meets the requirements for archival purposes or research set out in the PIPA Regulation and it is not reasonable to obtain the individual's consent.

The situations in which a PRO may collect personal information without consent must closely follow the exceptions in section 14 of PIPA.

3.4 Using Personal Information

3.4.1 We will only use personal information for purposes that are reasonable [for the purposes identified in [Article 3.3.2](#) or as permitted under [Article 3.4.2](#)] and we will only use personal information that is reasonable to carry out those purposes.

3.4.2 We will only use personal information without the individual's consent for the purposes in [Article 3.3.5](#) and for the following additional purpose:

- if the information is necessary to respond to an emergency that threatens the life, health or security of an individual or the public; or

The situations in which a PRO may use personal information without consent must closely follow the exceptions in section 17 of PIPA.

3.5 Disclosing Personal Information

3.5.1 We will only disclose personal information for purposes that are reasonable [for the purposes identified in [Article 3.3.2](#) or as permitted under [Article 3.5.2](#)] and will only disclose personal information that is reasonable to carry out those purposes.

3.5.2 We will only disclose personal information without the individual's consent for the purposes in Articles [3.3.5](#) and [3.4.2](#) and for the following additional purposes:

- when a treaty requires or allows for disclosure without consent and the treaty is made under an act or regulation of Alberta or Canada;
- to comply with a subpoena, warrant or order issued by a court or person or body having jurisdiction to compel the production of information or with a rule of court relating to the production of information;

- to a public body (under the *Freedom of Information and Protection of Privacy Act*) or to help in an investigation or a law enforcement proceeding;
- to contact next of kin or a friend of an injured, ill or deceased individual; or
- to the surviving spouse or adult interdependent partner (e.g. a same sex partner) or to a relative of an individual who has died if, in our opinion, the disclosure is reasonable.

A PRO should review any provision in its own statute, regulations, bylaws or rules that deals with disclosure of personal information without consent and make sure that the disclosure provisions in the Code closely follow the exceptions in section 20 of PIPA.

3.6 Collecting, Using and Disclosing Personal Employee Information

- 3.6.1 We may collect, use and disclose personal employee information without the individual's consent when it is reasonably required for the purposes of establishing, maintaining or terminating an employment relationship with the individual or to decide whether to hire a potential employee.
- 3.6.2 We will only collect, use and disclose personal employee information when it is reasonable for the particular purpose and we will limit the personal information collected, used or disclosed to that related to the employment or volunteer work relationship.
- 3.6.3 We may disclose personal employee information without the individual's consent to another organization when the individual is employed by the other organization or the other organization is collecting personal information to recruit a potential employee.

This provision should be used only if the PRO will disclose personal employee information without consent. If a PRO decides it will disclose the information without consent, it is suggested that the PRO establish a policy stating this.

- 3.6.4 Before we collect, use or disclose personal employee information about current employees without consent, we will notify the current employee that the information is going to be collected, used or disclosed and of the purposes for the collection, use or disclosure.
- 3.6.5 Personal information of employees can also be collected, used and disclosed without the individual's consent under the circumstances in Articles [3.3.5](#), [3.4.2](#) and [3.5.2](#).

The provisions for collecting, using and disclosing personal employee information should only be used if the Code is to apply to employees of the PRO.

3.7 Giving Access to and Correcting Personal Information

- 3.7.1 Upon request, we will give an individual or his or her authorized representative (an “applicant”) access to his or her personal information in a record that is in our custody or under our control. We will also let the applicant know what the information is being used for and how and under what situations the information is being or has been disclosed by us.

A PRO may specify the manner in which an access request is to be made. If a PRO has more than one office, section 8 of the PIPA Regulation permits the PRO to designate the office to which access requests should be sent. Section 10 of the PIPA Regulation allows PROs to accept access requests in alternative formats if the applicant is not able to make a request in writing.

- 3.7.2 If we do not have an actual record of the persons or organizations that the applicant’s personal information has been disclosed to, we will tell them who or what organizations their information may have been disclosed to.
- 3.7.3 We may require an applicant to give us evidence of his or her identity so we can ensure that the applicant has the right to access the personal information requested but we will only use such information for the purpose of identification and authentication.
- 3.7.4 We will act reasonably in searching for an applicant’s personal information and will respond to an applicant openly, accurately, and completely, and within 45 calendar days from receiving the request.

Section 31 of the Act permits a PRO to extend the time period for responding to a request for up to an additional 30 days, or for a longer period with the Commissioner’s permission, if the PRO does not have enough detail to identify the information requested, there is a large amount of information requested or to be searched, meeting the time limit would unreasonably interfere with the operations of the PRO, or more time is needed to consult with another organization or public body to determine if access can be given. If a PRO considers such a provision is necessary, it should be included in the Code.

3.7.5 We may charge the following fee(s) for processing the request.

The fee(s) charged must be reasonable. The PRO should specify what the amount of fee(s) will be or refer the reader to where the information about fees may be found, such as in a brochure or on its web site.

A PRO cannot charge a fee to process a request for personal employee information.

3.7.6 We will provide the applicant with a written estimate of the fee(s) being charged for processing the request. The time limit for processing the request stops once the fee estimate is sent to the applicant and does not recommence until the applicant has accepted the estimate and a deposit, if required, has been paid.

3.7.7 If an applicant does not respond to the free estimate within 30 days from which the estimate was sent, we will consider the applicant's request for access to have been withdrawn.

3.7.8 We may decline to provide the applicant with the information requested until the total fee payable is paid.

3.7.9 Members, employees and members of the public may seek access to their personal information by contacting _____ [position name or title] at _____ [contact information].

Do not include a reference to employees and members of the public if it is not intended that the Code apply to those persons.

3.7.10 We may refuse access to all or part of an applicant's personal information in the following situations:

- the information is protected by any legal privilege;
- the disclosure of the information would reveal confidential commercial information and it is not unreasonable to withhold the information;
- the information was collected for an investigation or legal proceeding;
- the disclosure of the information might result in that type of information no longer being supplied and it is reasonable that the type of information be supplied; or

If this exception applies to your PRO, you should specify in the Code the types of information that would no longer be supplied if access were permitted.

- the information was collected by a mediator or arbitrator.

If this exception applies to your PRO, you should clearly indicate the role of a mediator or arbitrator in your organization, for example, a mediator or arbitrator that is involved in an alternative dispute resolution mechanism for complaints of unprofessional conduct.

- 3.7.11 If we are reasonably able to sever the confidential commercial information to which the exception in [Article 3.7.10](#) applies, we will give access to the remainder of the information in the record.
- 3.7.12 We will refuse access to all or part of an applicant's personal information in the following situations:
- the disclosure of the information could reasonably be expected to threaten the life or security of another individual;
 - the information would reveal personal information about another individual; or
 - the information would identify the individual who gave an opinion in confidence about another individual and the individual who gave the opinion does not consent to the disclosure of his or her identity.
- 3.7.13 If we are reasonably able to sever the information to which the exceptions in [Article 3.7.12](#) apply, we will give access to the remainder of the information in the record.
- 3.7.14 We may require an applicant to view a copy of the record instead of examining the original record if the examination would unreasonably interfere with our operations, may result in harm to or destruction of the record, or may result in the disclosure of information to which access is not permitted or is refused under this Code.

A copy of the record cannot include information to which access would not be permitted or is refused under the Code.

- 3.7.15 We will inform the applicant if he or she will be given access to all or part of his or her personal information. If access is to be given, we will inform the applicant of when access will be given. If access to all or part of the applicant's personal information is refused, we will inform the applicant of the reasons for refusal and the specific exception(s) to the right of access contained in the Article(s) of this Code on which the refusal is based. We will also inform the applicant of the name of the person in our organization who can answer questions regarding the refusal, and of the applicant's right to ask the Commissioner for a review of our decision to refuse access.

A PRO can also establish in its Code that an individual can request to either examine the original record or obtain a copy of the record containing his or her personal information. A PRO must create a record for the individual from information it has in an electronic form if the record can be made with normal computer hardware, software and technical expertise, and creating the record would not unreasonably interfere with the operations of the PRO.

- 3.7.16 If an individual believes that his or her personal information in our custody or under our control has a mistake in it or is missing some information, he or she may request that we correct the information.
- 3.7.17 If we decide that the information should be corrected, we will do so as soon as reasonably possible. If it is reasonable to do so, we will send the corrected information to every organization that our records show has received the wrong information.
- 3.7.18 If we decide not to correct the information, we will make a note on the individual's personal information indicating that a correction was requested.
- 3.7.19 We will not correct or change an opinion, including a professional or expert opinion. We will make a note on the individual's personal information indicating that a correction was requested.

3.8 Accuracy

- 3.8.1 We will ensure that personal information used or disclosed by us will be sufficiently accurate, complete and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about an individual.
- 3.8.2 We will update personal information about members and employees as and when necessary to fulfill the identified purposes or upon notification by the individual.

Do not include a reference to employees if it is not intended that the Code apply to employees of the PRO.

3.9 Protection

- 3.9.1 We will use reasonable security safeguards to protect personal information against such risks as loss or theft, unauthorized access, disclosure, copying, use, modification or destruction. We will protect personal information regardless of the format in which it is kept and used.
- 3.9.2 We will protect personal information using physical, administrative and technical safeguards that are appropriate to the sensitivity of the information.

A PRO may wish to refer to the policies and procedures that specify the actual physical, administrative and technical safeguards that it has put in place to protect personal information.

3.10 Retention

- 3.10.1 We will keep personal information only as long as it remains necessary or relevant for the identified purposes or as required by law.

A PRO may wish to state in policy that, where personal information has been used to make a decision about an individual, it will retain that information for a period that is sufficient to allow the individual access to either the actual information or the rationale for making the decision.

A PRO should specify the retention periods for the different types of personal information that it holds, for example:

- registers of members are kept for X number of years;
- information about employees is kept for Y number of years;

or indicate where information about retention of records can be found.

- 3.10.2 We will maintain reasonable and systematic controls, schedules and practices for the retention and destruction of personal information in our custody or under our control. We will retain personal information for as long as it is reasonably required for the purposes identified in this Code or for legal purposes. When the personal information is no longer reasonably required for those purposes, we will destroy or erase the information or make it anonymous.

A PRO may wish to refer to the policies and procedures it may have regarding records management, retention and disposal/destruction.

4 Procedure For Handling Complaints

- 4.1 An individual who believes that _____ [name of PRO] has not complied with this Code has the right to make a written complaint about the matter to our organization. We will use our internal complaint-handling procedure to investigate and attempt to resolve the matter. Our internal complaint-handling procedure is as follows:

Articles [4.4](#), [4.5](#) and [4.7](#) to [4.10](#) set out the general components of a complaint-handling procedure but a PRO should set out the actual details of its complaint process here.

- 4.2 An individual always has the right to make a complaint to the Information and Privacy Commissioner or to ask the Commissioner to review a decision we have made. However, individuals are encouraged to use our internal complaint-handling procedure first.

- 4.3 We will make our complaint-handling procedure readily accessible to individuals. We will provide brochures or include information on our web site about how to lodge a complaint, the time within which a complaint will normally be handled, and the fact that complaints will be handled by an officer of our organization with appropriate authority to deal with the complaints.

The actual contact information of the officer within the PRO handling complaints could be included here.

It is preferable for the officer within the PRO that is investigating complaints to be someone other than the designated compliance officer.

- 4.4 We will provide the complainant with appropriate assistance to ensure that the complainant has equitable access to the complaint-handling procedure.

- 4.5 We will provide the complainant with a copy of this Code, together with any explanatory materials or policies, upon request.

- 4.6 We may decide not investigate a complaint if:

- the complaint relates to an act or practice that is not a possible breach of the privacy of an individual;

- the complaint relates to an act or practice that is no longer reasonably able to be investigated because of the length of time since it occurred;
- the act or practice relates to an event which occurred prior to the organization being subject to this Code;
- the complaint is trivial, frivolous or vexatious; or
- the complaint relates to an act or practice that is the subject of court proceedings that have commenced or are intended to be commenced.

4.7 With the exception of complaints that we have decided not to investigate as in [Article 4.6](#), we will investigate and respond to all complaints within a reasonable period of time [or within x number of days]. If the complaint is found to be justified, we will take appropriate steps to resolve the complaint including, if necessary, amending our policies and procedures (or this Code).

4.8 A complainant will be expected to provide full details of how the complaint arose, including the identification of the parties involved, if known, copies of any relevant documentation and reasons why the complainant believes his or her privacy may have been breached.

4.9 A complainant may be represented by a legal practitioner or other advocate.

4.10 We will inform the complainant of the outcome of the investigation regarding his or her complaint.

5 Monitoring/Reviewing the Operation of the Code

5.1 We will monitor compliance with this Code.

5.2 Our Governing Council [or other name of the governing body of the PRO] will appoint a person to review this Code at regular intervals [e.g. every 3 years] to ensure that the Code is still serving its stated purposes; that it is being complied with; that the internal complaint-handling procedure is still effective; and to determine if there are any amendments that should be made to improve the operation of the Code.

5.3 We will ensure that there are sufficient resources allocated to conduct these reviews.

5.4 The person appointed to review the Code will report his or her findings and recommendations to the Governing Council.

A PRO may establish a policy of sending a copy of the report to the Office of the Information and Privacy Commissioner but PIPA does not require this.

6 Establishing the Code

- 6.1 This Code is approved by our Governing Council [or other name of the governing body of the PRO] in accordance with [name the legislative instrument used by the PRO's governing body to pass this Code].

The Code must include provisions relating to the way the Code is established by the PRO.

7 Publication of the Code

- 7.1 We will publish this Code in a brochure [specify which printed format the Code will be published in] and on our web site.

A PRO must state in the Code that it will publish the Code in printed or electronic form.