ENGINEERS & GEOSCIENTISTS BRITISH COLUMBIA

POLICY

POLICY	Engineers and Geoscientists BC Privacy Policy
NUMBER OF POLICY	CO-18-44
DATE OF POLICY	June 15, 2018
APPROVED BY	The Board

PURPOSE

Engineers and Geoscientists BC ("**Association**") must collect, secure, use, and disclose information in accordance with its enabling statute, the *Engineers and Geoscientists Act* ("**EGA**"), and also the *Freedom of Information and Protection of Privacy Act* ("**FIPPA**"), which is a statute that applies to all public bodies in British Columbia.

The purpose of this Privacy Policy is to establish principles and general processes for the Association to fulfill its relevant statutory obligations, in accordance with the best practices recommended by the Office of the Information and Privacy Commissioner for British Columbia ("**OIPC**"). This Privacy Policy is not intended as a detailed procedure manual for Association employees and other individuals who handle information on the Association's behalf. From time to time, security protocols for the handling of information in specific areas of operation will be developed and used under this Privacy Policy (see section 14 below).

DEFINITIONS

In this Privacy Policy:

"personal information" refers to recorded information about an identifiable person other than contact information.

"contact information" refers to information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual.

"confidential information" refers to personal information and other types of information in the Association's control or possession that is not publicly available.

GOVERNANCE

Head

FIPPA requires the Association to designate a person to serve as the Association's "Head" for the purposes of FIPPA. Under this Privacy Policy, the Head refers to the individual designated by the Board to fulfill that role. In the event that at any time the designated individual ceases or is unable to serve as Head, and if the Board does not designate another individual to that role, then the Registrar will serve as and fulfill the duties of Head.

Privacy Officer

The Head may designate and delegate to an appropriately qualified Association staff member ("Privacy Officer") responsibilities for ensuring the Association's compliance with FIPPA.

Information Security Officer

The Head may designate and delegate to an appropriately qualified staff member within the Association's Information Systems Department ("Information Security Officer") responsibilities for the implementation and ongoing administration of the Association's information security program.

Compliance Report

From time to time, as circumstances may demand, taking into account changes in the Association's operations, technology, and the law, the Head will:

(a) assess the resources available and needed to ensure the Association's compliance with FIPPA and the upkeep of its good practices in terms of monitoring and improving its privacy management program, and the Head will apprise the CEO and Registrar of the results of the assessment;

(b) arrange for an internal or external audit of the Association's privacy management program; and

(c) annually report to the CEO and Registrar on the status of the Association's privacy management program.

PERSONAL INFORMATION DIRECTORY

The Association's Departments will collaborate in the preparation and maintenance of an updated personal information directory ("Directory") that accounts for the Association's personal information banks.

In accordance with section 69(6) of FIPPA, the Directory will include the following information with respect to each personal information bank that is in the control or possession of the Association:

(i) its title and location;

(ii) a description of the kind of personal information and the categories of individuals whose personal information is included;

(iii) the authority for collecting the personal information;

(iv) the purposes for which the personal information was obtained or compiled and the purposes for which it is used or disclosed; and

(v) the categories of persons who use the personal information or to whom it is disclosed.

Upon request, the Head or Privacy Officer will make the Directory publicly available for inspection and copying.

COLLECTING PERSONAL INFORMATION

Unless otherwise authorized by law, the Association will communicate the purposes for which it collects personal information before or at the time of collection. The communication may be oral or in writing.

The Association will collect personal information directly from the subject individual, unless the individual authorizes collection from another source or if collection from another source is authorized by law.

Personal information that the Association may collect in the ordinary course from an applicant or member includes the following:

1. name;
2. date of birth;
3. citizenship and residency status;
4. home address, telephone number, and email address that is private and not used by the applicant or member for business purposes;
5. educational background, professional experience, employment history, criminal and disciplinary history, and other personal information relevant for registration;
6. personal information relevant for reviewing or investigating a complaint against the member;
7. personal information relevant for conducting a practice review of the member;
8. personal information relevant for providing professional practice advice to the member;
9. personal information relevant for the member's participation in the organizational quality management program, or other non-mandatory professional programs; and
10. personal information relevant for the member's appointment to serve in an official function under the EGA or the bylaws of the Association, or otherwise serve as a volunteer for the Association or act on behalf of the Association.

The purposes for which the Association collects personal information about applicants and members include the following:

A. verify the identity of applicants;

B. assess whether applicants meet the requirements for professional licensure;

C. communicate with applicants or members;

D. maintain the Association's register in accordance with section 19 of the EGA;

E. renew licenses;

F. investigate complaints against members pursuant to sections 29 and 30 of the EGA;

G. provide certificates, professional seals, and educational materials to members;

H. process resignations;

I. operate an awards program;

J. conduct practice reviews in accordance with the bylaws of the Association;

K. provide professional practice advice to members;

L. allow members to participate in non-mandatory professional programs, such as the organizational quality management program; and

M. select and appoint members to serve in official functions under the EGA or the bylaws of the Association, or otherwise serve as volunteers for the Association or act on behalf of the Association.

The Association will routinely collect personal information from individuals who are not applicants or members, including employees, volunteers, and complainants. However, the Association will only collect personal information that is necessary or related to it fulfilling its duties and objects under the EGA.

CONSENT

The Association will obtain consent to collect, use, or disclose personal information about any individual, unless the Association is authorized under the EGA and/or FIPPA to make such collection, use, or disclosure without the individual's consent.

Consent may be obtained orally or in writing, or it may be implied where the purpose for collecting, using, or disclosing the relevant personal information is consistent with, and reasonably and directly connected to, a valid purpose for which an individual has already provided consent.

In the event that the Association seeks to use personal information it has already collected for a new purpose which is substantially different from the original purpose for which the personal information was obtained, the Association will seek consent from the subject individual for the new purpose.

The Association will obtain a member's consent before sharing any personal information with an Association Affinity Benefits Partner that offers special discounts or promotions to Association members.

Individuals may withhold or withdraw their consent for the Association to use their personal information, subject to certain exceptions under FIPPA in connection with the Association's role as a licensing and law enforcement body. An individual's decision to withhold or withdraw consent to certain uses of personal information may restrict the Association's ability to provide a particular service to the individual, about which the Association may advise the individual at the time that the individual communicates a decision to withhold or withdraw consent.

The Association will only disclose personal information pursuant to section 25 of FIPPA, with the knowledge and decision of the Head.

The provisions of section 25 of FIPPA are the following:

> ***25*** *(1) Whether or not a request for access is made, the head of a public body must, without delay, disclose to the public, to an affected group of people or to an applicant, information*
>
> *(a) about a risk of significant harm to the environment or to the health or safety of the public or a group of people, or*
>
> *(b) the disclosure of which is, for any other reason, clearly in the public interest.*
>
> *(2) Subsection (1) applies despite any other provision of this Act.*
>
> *(3) Before disclosing information under subsection (1), the head of a public body must, if practicable, notify*
>
> *(a) any third party to whom the information relates, and*
>
> *(b) the commissioner.*
>
> *(4) If it is not practicable to comply with subsection (3), the head of the public body must mail a notice of disclosure in the prescribed form*
>
> *(a) to the last known address of the third party, and*
>
> *(b) to the commissioner.*

The Association will not disclose personal information pursuant to section 25 of FIPPA, without the knowledge and decision of the Head.

ACCESS TO PERSONAL INFORMATION

Individuals have a right to access personal information about them that is in the possession or control of the Association, except insofar as access may:

(a) interfere with a regulatory process, such an investigation or hearing;

(b) reveal the identity of another person who provided information to the Association on a confidential basis;

(c) unreasonably invade another person's personal privacy;

(d) place an individual's health or safety at risk or constitute a risk to public health and safety;

(e) reveal information that is privileged; or

(f) reveal information that the Association is required or entitled to withhold from disclosure under FIPPA or by the operation of law.

A request to access personal information must be in writing and must be sufficiently detailed in that it identifies the personal information being sought. Where the Association receives any such request, the Association staff member who receives the request will without delay bring the request to the attention of the Privacy Officer or Head. The request will then be considered and responded to by the Privacy Officer or Head in accordance with the requirements of FIPPA.

ACCURACY AND CORRECTION OF PERSONAL INFORMATION

The Association will make reasonable efforts to ensure that any personal information in its possession and control is accurate and complete if that personal information may be used to make a decision about an individual or if it might be disclosed to other persons.

For the purpose of ensuring accuracy and completeness of personal information about an individual, that individual may make a request to the Association for the correction of the individual's personal information. The request must be in writing and must sufficiently identify the personal information in issue and any correction sought.

Where the Association receives a written request from an individual for the correction of the individual's personal information, the Association staff member who receives the request should without delay bring the request to the attention of the Privacy Officer or Head, for one or both of them to assess the merits of the request and respond to it. In the event that the Privacy Officer or Head determines that inaccuracy or incomplete information exists concerning the personal information that is in issue, the Privacy Officer or Head will direct that the Association make appropriate corrections to its records to ensure that the personal information in issue is made accurate and complete.

The Association may refuse to correct personal information in the manner requested by an individual in the following circumstances:

(a) the individual requesting the correction does not provide sufficient information to enable the Association to assess the merits of the request;

(b) the Privacy Officer or Head determines that there is no existing record in the Association's possession or control which contains any relevant personal information;

(c) the Privacy Officer or Head determines that there is no error in any records in the Association's possession or control that requires correction;

(d) correction may alter an original document that belongs to another person;

(e) correction may alter an original document that the Association or another person may require in a Court or administrative proceeding;

(f) correction may interfere with the Association's regulatory processes, including an inquiry, investigation, or hearing;

(g) correction may interfere with another regulatory body's or law enforcement agency's regulatory or enforcement activities; or

(h) the Privacy Officer or Head reasonably believes that correction may be prohibited by law.

RETENTION AND DISPOSAL OF PERSONAL INFORMATION

Pursuant to the requirements of section 31 of FIPPA, the Association will retain personal information for at least one year after that personal information is used to make any decision that directly affects an individual the personal information is about.

The Association, and any person holding personal information on behalf of the Association, will retain and dispose of personal information in a manner that ensures that records containing the personal information will not be accessible to any person after the disposal.

The Director of each of the Association's Departments will ensure that appropriate processes practices are in place for the Department's secure retention of all records containing personal information that are in the Department's possession or control.

CONFIDENTIALITY AGREEMENTS, AUTHORIZATION AND TRAINING

The Director or Associate Director of each of the Association's Departments will ensure that each employee, contractor, or volunteer who may access or handle confidential information in the Department's care:

I. will agree in writing to follow confidentiality measures appropriate for that individual's discharging of the individual's specific duties, unless the individual is already under a formal obligation to appropriately preserve confidentiality;

II. will not gain access to the Association's information systems, prior to the individual being authorized in accordance with the Association's information security authorization process; and

III. is offered and receives training appropriate for the individual's specific role in accessing and handling confidential information.

From time to time, having regard to any significant changes in the Association's operations or information systems, the Privacy Officer and/or Head will arrange for organizational-wide privacy training relevant for reducing risks of privacy breaches.

PRIVACY COMPLAINT

The Association will assess and respond to any complaint from any individual that concerns the Association's compliance with FIPPA and this Privacy Policy. Any Association staff member who receives such a complaint will without delay bring the complaint to the attention of Head or Privacy Officer. The Head or Privacy Officer will assess the merits of the complaints and will directly communicate with the complainant to address the relevant issues raised by the complainant.

BREACH AND INCIDENT MANAGEMENT RESPONSE

Where an Association staff member becomes aware of an instance of unauthorized access or disclosure of confidential information, the Association staff member will without delay bring that incident to the attention of the Head, Privacy Officer, or Information Security Officer. Having regard to the significance of the incident, the risks to any person, and the Association's obligations under FIPPA, the Head, Privacy Officer, and/or the Information Security Officer will, to the extent appropriate and necessary, do as follows:

(a) direct that the Association take active steps to stop any continued unauthorized access or disclosure of confidential information that is foreseeable and connected to the incident;

(b) direct that the Association take active steps to reduce the adverse impact of the incident on affected persons; and

(c) report the incident to the OIPC.

Where there is an incident of significant unauthorized access or disclosure of confidential information, the Privacy Officer and/or Head will investigate the causes of the incident and will direct that the lessons learnt from the investigation are incorporated into procedures, practices, and training for the Association's staff members.

RISK ASSESSMENT TOOLS

The Association will conduct a privacy impact assessment ("**PIA**") whenever:

(a) there is a significant modification of an existing Association system, program or activity that may impact the collection, use, and disclosure of personal information; or

(b) the Association is undertaking a new project involving the collection, use, or disclosure of personal information.

In the event that any of the Association's Departments undertakes either of (a) or (b) directly above, the Director or Associate Director of that Department will prepare a PIA, in consultation with the Head, Privacy Officer, and/or the Information Security Officer.

SECURITY PROTOCOLS

The Association is committed to ensuring the security of confidential information in its possession and control, in order to protect the confidential information from unauthorized access, collection, use, disclosure, copying, modification and disposal.

From time to time, and on an ongoing basis, taking into account changes in the Association's operations, technology, and security concerns, the Association will create and update security protocols for the protection of confidential information in the Association's possession and control.

The security protocols will be made available in writing to the Association's staff members as they are created and updated. The security protocols will include standards, procedures and instructions relevant for the storage, usage, movement, transmission, and deletion of confidential information in all of the Association's operational processes. The security protocols will address the following issues:

1. the classification of various types of confidential information, including personal information and credit card cardholder data;
2. the identification of the location of confidential information (physically and electronically);
3. the identification of which individuals are responsible for authorizing access to specific types of confidential information;
4. the identification of operational and business processes that create, acquire, store, utilize, move/transmit, or delete confidential information;

5. the physical security of the Association's offices, facilities, and information systems;
6. the Association's requirements for volunteers and contractors physically securing confidential information that they hold in their possession on behalf of the Association;
7. the electronic security for the protection of confidential information stored, accessed, transmitted to/from or deleted within the Association's information systems;
8. the Association's electronic security requirements for volunteers and contractors;
9. the methods for remotely accessing the Association's information systems; and
10. the timing of the destruction of various types of confidential information.

REVIEW DATES

June 15, 2018 (CO-18-44) – Approved by Council