ARCHITECTURAL INSTITUTE OF BRITISH COLUMBIA

Privacy Policy

1.0 Background and Authority

1.1 The AIBC is designated as a local public body under the *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165 (FIPPA).

1.2 The AIBC's accountability for the collection, use, disclosure of, and access to, personal information is established under the FIPPA, AIBC Bylaws under the *Professional Governance Act*, S.B.C. 2018, c. 47 (the "PGA"), and other statutes where applicable.

1.3 The Registrar is designated as the head of the AIBC for the purposes of the FIPPA, as per the Bylaws.

2.0 Purpose

2.1 The AIBC has ethical and legal obligations for the control or custody of personal information about Registrants, contacts including applicants and the public, and employees/contractors. The purpose of this Compliance Policy ("Policy") is to establish how the AIBC complies with these obligations and demonstrates accountability for managing this information, in a way that respects the privacy of individuals while allowing the AIBC to fulfill its regulatory mandate effectively.

3.0 Scope of the Policy

3.1 This Policy describes the AIBC's policies and processes for complying with the FIPPA requirements related to:

- collection, use, and disclosure of personal information, including notification requirements;
- accuracy and correction of personal information;
- protection of personal information; and
- retention and disposal of personal information.

3.2 This Policy also responds to section 36.2 of the FIPPA and related ministerial directions, requiring a privacy management program, which includes the following components, in addition to the items listed in paragraph 3.1 of this Policy:

- a process for conducting privacy impact assessments;
- a publicly-available personal information directory;
- a process for responding to freedom of information (FOI) requests;

- a process for responding to privacy breaches; and
- employee privacy awareness and education.

4.0 Collection, Use, and Disclosure of Personal Information

4.1 Collection of Personal Information

4.1.1 The AIBC collects personal information directly from the subject individual, except in limited circumstances under the FIPPA (section 27) or if collection from another source is authorized by law.

4.1.2 The AIBC collects personal information from Registrants to conduct regulatory functions, including but not limited to:

- administering regulatory programs and services, including processing applications for registration and reinstatement; investigating complaints; processing continuing education reports, course and examination registrations; and delivering professional development opportunities and practice advice;
- collecting and processing payments;
- maintaining a publicly-available register (Registrants and Former Registrants);
- enabling the Board, Committees, and operational advisory groups to carry out their regulatory functions; and
- communicating with Registrants regarding regulatory and non-regulatory matters

4.1.3 The AIBC collects the personal information of employees/contractors to manage and compensate them during their engagement and for appropriate record keeping post-employment, and of employment applicants for effective recruitment and selection.

4.1.4 The AIBC may also collect personal information from volunteers, applicants, and members of the public for the purposes of delivering programs and services including, investigating complaints and illegal practice matters, practice advice, processing applications and event registration, and communicating AIBC activities.

4.2 Collection Notification

4.2.1 The AIBC provides notification when personal information is collected directly from an individual, which notice includes:

- the purpose for which the information is being collected;
- the legal authority under which the information is being collected; and

- the contact information of a designated officer or AIBC department who can answer questions regarding the collection.

4.3 Use and Disclosure of Personal Information

4.3.1 The AIBC controls and monitors access and use of personal information.

4.3.2 The AIBC uses and discloses personal information in its custody or under its control:

- for the purpose for which the information was obtained or compiled or for a consistent purpose;
- in the manner to which an individual has consented;
- as permitted or required by the FIPPA, the PGA, the AIBC Bylaws, or as authorized or required by other law; and
- to conduct the regulatory and administrative functions identified in paragraphs 4.1.2-4.1.4.

4.3.3 The CEO & Registrar, Deputy CEO, and Deputy Registrars have the authority to request that an employee access and/or disclose the personal information of an Individual Registrant or non-registrant.

4.3.4 Employees are provided access to personal information on a 'need to know' basis in order to perform their job functions and responsibilities, and when it is necessary to carry out AIBC operations and activities.

4.3.5 Requests from third parties for disclosure of personal information under section 5 of the FIPPA will be processed as indicated under heading 10.0 of this Policy.

4.3.6 Disclosure of Registrant, non-registrant, or employee personal information by the AIBC in emergency or compelling circumstances will be made in accordance with provisions of the FIPPA.

5.0 Accuracy and Correction of Personal Information

5.1 The AIBC takes all reasonable steps to ensure the accuracy and completeness of any personal information collected or recorded and is diligent in avoiding errors due to carelessness or other oversights. Employees verify the accuracy of personal information against reliable sources when necessary. During collection, individuals are asked to confirm the accuracy of their information.

5.2 Individuals are provided with opportunities to update their personal information at regular intervals where appropriate, such as information about Registrants and employees. If an individual identifies that their personal information is inaccurate or incomplete, they may request correction, as per section 29 of the FIPPA. Employees will promptly correct or update the information as soon as they are discovered or reported and inform any parties to whom the inaccurate or incomplete information has

been disclosed. If the correction cannot be made, a note of the requested correction must be added to the file.

6.0 Protection of Personal Information

6.1 The AIBC is committed to maintaining the security of personal information and other sensitive information, including implementing appropriate security safeguards for its computer and network systems.

6.2 The AIBC undertakes regular reviews to update security policies and controls as technology changes to ensure ongoing personal information security.

6.3 The AIBC completes privacy impact assessments (PIA) for any proposed or significantly revised system, project, program or activity prior to implementation, in accordance with the FIPPA, and heading 8.0 of this policy.

6.4 When the AIBC retains an external organization to undertake work on its behalf that involves the collection, use, disclosure, or disposal of personal information, the AIBC enters into an agreement that requires the organization to protect personal information in accordance with the FIPPA and AIBC expectations appropriate to the nature of the services.

6.5 AIBC volunteers are required to adhere to a confidentiality and protection of privacy policy to help ensure that AIBC information they may have access to in the course of their volunteer duties is managed in a way that respects privacy.

6.6 The AIBC has a responsibility to protect against unauthorized access and disclosure of personal information, including ensuring that access or disclosure is only made to or by authorized individuals, and that reasonable measures are taken to prevent any unauthorized access, disclosure, loss, or theft of information. Proper handling of personal information therefore includes the following practices:

- hard copies of files and records containing personal information are kept in a secure location, preferably where locked and secured against theft or unauthorized access;
- available security systems (e.g., locking offices when not in use, activating alarm systems and posting security) are utilized;
- discussing personal information in public areas where third parties may overhear or view records containing personal information is avoided;
- removal of records containing personal information from AIBC premises is prohibited except as necessary, and, in such cases the records are kept in a secure location and not exposed to risk of loss, theft or unauthorized access;

- measures to protect against loss or theft of personal information are in place, including enhanced security of electronic or hard copies of personal information that may be vulnerable to theft or loss; and

- any potential or actual privacy breach is reported immediately, and according to the Privacy Breach Reporting Policy.

7.0 Retention and Disposal of Personal Information *(Note: Detailed retention and disposal schedules are under development.)*

7.1 Retention of Personal Information

7.1.1 Personal information is retained for as long as required by law, and for a minimum of one year after it has been used to make a decision that directly affects the individual to whom the information pertains, in accordance with the FIPPA.

7.1.2 Personal information is retained beyond the minimum retention period if it is required for operational, legal, or archival purposes.

7.1.3 Retention schedules are clearly documented, and deviations are approved by the appropriate authority.

7.2 Disposal of Personal Information

7.2.1 Personal information that is no longer required for operational, legal, or archival reasons is disposed of securely and promptly. The timing and method of disposal is consistent with legal and regulatory requirements.

7.2.2 Records of disposal, including the date and method, are maintained.

7.2.3 Personal information in hardcopy form is shredded or otherwise destroyed in a manner that ensures it cannot be reconstructed or read.

7.2.4 Personal information in electronic form is permanently erased using industry-standard methods to ensure it cannot be recovered. Special procedures are followed to remove data from electronic devices before disposal or redeployment.

8.0 Privacy Impact Assessment

8.1 A Privacy Impact Assessment ("PIA") is completed and approved by the privacy officer before implementation or significant change to any program or system that requires the collection, use, or disclosure of personal information.

9.0 Personal Information Directory

9.1 Section 69(6) of the FIPPA requires the AIBC to make available for public inspection and copying a personal information directory that lists the AIBC's personal information banks (PIBs). The purpose of making this information available is to help the public know what personal information is in custody of the AIBC.

9.2 The personal information directory describes the types of personal information that the AIBC collects, uses, retains, and discloses, along with the legal authority to do so. The directory includes:

- the title of each personal information bank;
- a description of the kind of personal information and the categories of individuals whose personal information is included;
- the authority for collecting the personal information; and
- the purposes for which the personal information was collected or compiled and the purposes for which it is used or disclosed, and to whom.

9.3 The personal information directory is updated annually according to internal guidelines and is published on the AIBC website.

10.0 Freedom of Information (FOI) Requests

10.1 Requests for access to records under section 5 of the FIPPA must be made in writing, identifying the information sought, the authority for the request, and the reason for the request.

10.2 The AIBC will process access requests in accordance with the FIPPA.

10.3 The AIBC reserves the discretion to charge a fee for access request services in accordance with AIBC Bylaw 8.3 and the FIPPA.

10.4 Employees may be asked to assist the head of the local public body or privacy officer or others delegated with privacy tasks to assist in processing access requests.

11.0 Privacy Breaches

11.1 A breach of privacy includes unauthorized access to the AIBC's physical or electronic records, misdirected communications, including mail, and electronic communications, and the loss or theft of physical records and electronic records stored on portable data storage devices.

11.2 The AIBC complies with section 30.5 of the FIPPA, which requires an employee to immediately report an unauthorized disclosure of personal information to the head of the local public body, who is the Registrar in the case of the AIBC.

11.3 The AIBC will respond to an internal or external privacy breach according to the Privacy Breach Reporting Policy. The Policy supports the AIBC to effectively:

- Contain any incidents;
- Recover as much of the affected information as possible;
- Assess the harm/impact on affected individuals;
- Remediate the breach and minimize the harm/impact on affected individuals; and
- Prevent similar incidents from happening in the future by updating processes, practices, and policies as required, and delivering additional training and awareness.

12.0 Employee Privacy Awareness and Education

12.1 Employee privacy education activities that support the AIBC's compliance with the FIPPA is a required component of a privacy management program. All employees receive training, including but not limited to the following topics:

- FOIPPA Foundations: Privacy and Access Fundamentals Course
- FIPPA and employee protection of privacy obligations and responsibilities
- Personal information banks (PIBs)
- Handling a potential or actual privacy breach

12.2 Role-based training is also provided for activities related to: the Registrant database and acceptable use policies; access to information requests; and the role of the AIBC as a local public body with a public protection mandate, balanced with accountabilities under the FIPPA.