

	Policy No:  <p style="text-align: center;">4</p>	Approval Date: March 27 <sup>th</sup> 2019  Created: March 6 <sup>th</sup> 2019  Last Reviewed:
<p><b>Title:</b></p> <p style="text-align: center;"><b>Privacy and the Protection of Personal Information Policy</b></p>		
<p><b>Background &amp; Purposes:</b></p> <p>The purpose of the Privacy and the Protection of Personal Information Policy is to formalize and make public APSA’s current practice of protecting the confidentiality of information we collect about our members, without creating unreasonable impediments to the Association’s normal business.</p> <p>The <a href="#">BC Societies Act</a> requires APSA to keep a “register of members, organized by different classes of member if different classes exist, including contact information provided by each member.” Due to the nature of APSA, and its role as representative of its members to Simon Fraser University, the Association also requires job-related information about its members.</p> <p>APSA is an organization as defined by the <a href="#">Personal Information Protection Act of BC (PIPA)</a> and is subject to the provisions of the Act in the collection, usage, storage, and disclosure of information.</p>		

**Scope:**

This Policy applies to all personal information collected, used, disclosed, and retained in any form by APSA about APSA members and non-members (including employees, independent contractors, and other individuals involved with APSA).

The application of this Policy is subject to the requirements and provisions of applicable federal and provincial privacy legislation and any other applicable legislation or regulations. APSA may change the terms of this Policy from time to time and will make available any updated version of this Policy.

**Accountability and Transparency:**

APSA is accountable and responsible for maintaining and protecting personal information under its control.

To ensure accountability:

- All directors, employees, independent contractors, and volunteers are informed about this policy;
- APSA has designated a Privacy Officer who ensures day-to-day compliance with the Policy; and
- APSA will seek assurances regarding the privacy of personal information that has been transferred to a third party for use or processing, by requiring that those third parties safeguard all personal information as required by law.

The Executive Director is the Privacy Officer for APSA, and the Member Services Coordinator will be the alternate in his/her absence.

The duties of the Privacy Officer are but not limited to:

- Conducting a privacy audit and self-assessment
- Developing a privacy policy
- Implementing and maintaining a privacy policy
- Managing privacy training
- Responding to requests for access to and correction for personal information
- Working with the Office of the Information and Privacy Commissioner in the event of an investigation.

### **Collection, Use, and Disclosure of Personal Information:**

APSA may collect personal information using a variety of means, including written and verbal communications and through its website.

APSA may generally collect, use or disclose employee personal information for the reasonable purposes of establishing, managing or terminating the employment relationship between APSA and the employee. [employee is defined in PIPA to include volunteers]

APSA provides services to its members and represents them in all aspects of their relationship with their employer, Simon Fraser University.

Examples of the purposes for which APSA collects, uses, and discloses personal information includes, but is not limited to:

- To establish and maintain a record of APSA's membership;
- Conducting surveys of member preferences, needs, or interests;
- Collecting and managing dues;
- Communicating with members, such as providing information and responding to inquiries;
- Providing information about its membership for the purpose of the annual general meeting;
- To meet legal and regulatory requirements; and
- Investigating and resolving member issues, concerns and/or grievances.

On request, persons collecting personal information will elaborate on the purpose or object for such collection or refer the individual to the designated person who can do so.

APSA may also disclose personal information to third parties such as third party contractors with whom it has contracted to provide certain services. The third parties will have access to personal information needed to perform their functions, but are only provided the limited amount of information required to perform their services or functions. Examples of third party service providers APSA engages or may engage are but not limited to:

- Outside legal counsel to assist in the investigation of member issues, concerns, and/or grievances;
- Website hosting located in Canada;
- Virtual file server located in Canada;
- Email service providers located in the USA; and
- Accounting software which stores information in the cloud, located in the USA.

When APSA uses agents, suppliers and/or service providers, it requires them to protect personal information in accordance with the law and with the same or more stringent security and privacy standards than APSA. Any such disclosure of personal information by APSA to a third party will be conditional upon the information being used solely for the purpose for which it has been disclosed. If an individual does not wish APSA to provide their personal information to a third party, there may be situations where APSA will be unable to provide that individual with services.

#### **Consent:**

Individuals shall be informed and their consent obtained for the collection, use and disclosure of their personal information, except where otherwise required or permitted by law. When it is appropriate, the written consent of the individual shall be obtained (i.e. by mail or email). An individual's consent may also be obtained verbally or implied through their conduct with APSA.

APSA may periodically request written confirmation from an individual that the information collected and maintained by APSA is up to date and accurate. APSA, at its option, may also ensure that it has continuing consent to use and retain personal information.

APSA will disclose personal information, without notice and without consent, only if required to do so by law or in the good faith belief that such action is necessary.

Examples are:

- Seeking the consent of the individual might defeat the purpose of collecting the information, such as in the investigation of a breach of an agreement or law;
- It is clearly in the individual's best interest and notice or consent cannot be obtained in a timely manner;

- In the reasonable judgement of APSA, it appears that there is an imminent danger to life or property, which could be avoided or minimized by disclosure of the information to a public authority or agent of a public authority; and
- Information is provided to a lawyer representing APSA, to comply with a subpoena, warrant or other court order, or as may be otherwise required or authorized by law.

### **Retention of Personal Information:**

If personal information has been used to make a decision about a member or an employee, APSA will keep the personal information for at least one year after APSA has made that decision, to allow the individual to have access to it after the decision has been made. Subject to this one-year retention requirement, APSA will only retain personal information as long as necessary to fulfill the identified purposes, or for as long as required for legal or business purpose.

Examples of personal information APSA may keep for longer than one year are, but not limited to:

- Grievance and arbitration files which may have information which may be useful for future grievances or arbitrations.
- Grievance and arbitration files which may be useful in collective bargaining.
- Employee or volunteer files.

APSA will maintain controls, schedules, practices and procedures for retention and destruction of personal information.

### **Security of Personal Information**

APSA has implemented procedures to protect the privacy of personal information with safeguards appropriate to the sensitivity of the information.

APSA will safeguard personal information in its possession or control from loss or theft and from unauthorized access, use, disclosure, copying or modification through appropriate security measures depending on the sensitivity, format and storage of the personal information.

APSA's information security safeguards include, but are not limited to:

- Security of the premises;
- Locked file cabinets;
- Restricted access to files containing personal information;
- Technological safeguards such as security software and firewalls to prevent unauthorized computer or access; and
- Policy prohibitions against unauthorized use or disclosure.

As well, APSA will use care when destroying or disposing of personal information to prevent unauthorized access, use or disclosure of any personal information.

APSA's directors, employees, independent contractors, and volunteers with access to personal information are required to respect the confidentiality of such information.

### **Access to and Correction of Personal Information:**

APSA is open about this Policy and will make this Policy available to members, non-member participants, directors, employees, independent contractors, and volunteers, and to other individuals upon request. On request, APSA will also advise if and how an individual can access their personal information.

In order to obtain access to the personal information APSA has in its possession and control relating to an individual, that individual should make a written request to APSA's Privacy Officer. Employees can also seek access to their personal information by contacting APSA's Executive Director. The written request must provide sufficient detail to allow APSA to identify the personal information being sought. Unless exempted by law, APSA will provide the individual with access to his or her personal information under APSA's possession or control and an accounting of the collection, use and disclosure of his or her personal information.

Except for employee personal information, APSA may charge a minimal fee according to the cost required to retrieve and provide the requested information. APSA may provide an estimate of the fee in advance and in some cases, will require a deposit for all or part of the fee.

In some cases, APSA may not provide access to personal information that it holds about an individual. Examples of this include:

- Disclosing the personal information could reveal confidential information;
- If the personal information is protected by solicitor-client privilege;
- Where the denial of access is authorized by law;
- Where information relates to existing or anticipated legal proceedings against the individual making the request;
- Where the information is collected for purposes of an investigation or the information is the result of an arbitration or other formal dispute resolution process; or
- Where the request is frivolous or vexatious.

APSA will also not provide access to personal information that:

- Could reasonably be expected to threaten the safety or physical or mental health of an individual other than the individual who made the request;
- Could reasonably be expected to cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request;
- Would reveal personal information concerning another individual; or
- Would reveal the identity of an individual who has provided personal information concerning another individual and the individual providing the personal information does not consent to disclosure of his or her identity.

If APSA denies an individual's request for access to personal information, it will advise the individual of the reason for the refusal, and will provide the name, title, and contact information of the designated person who can address the refusal.

APSA will use reasonable efforts to ensure that personal information is accurate and complete for the purposes for which it is to be used. An individual is permitted to challenge the accuracy and completeness of their personal information and, in appropriate circumstances, APSA will amend its records. Any differences as to accuracy or completeness that cannot be resolved will be noted in the individual's file, if applicable.

**Compliance:**

APSA also ensures that any of its staff and volunteers who deal with personal information are properly trained and are aware of the necessary and appropriate measures required to protect personal information. APSA staff, board, and committee members sign confidentiality statements to this effect.

**Concerns, Inquiries and Requests:**

Any concerns, inquires or requests related to APSA's treatment of personal information, including access to personal information, should be directed to APSA's Privacy Officer as follows:

Andrew Boden

APSA Office – AQ 5133  
8888 University Drive  
Burnaby BC, V5A 1S6

778-782-5423

[apsa@sfu.ca](mailto:apsa@sfu.ca)