



SFSS Privacy and
Information
Management
Policies

Simon Fraser Student Society

simon fraser

student society

TABLE OF CONTENTS

Purpose of These Policies.....	3
Policy Review and Approval Process	4
P-1: Personal Information and Privacy Policy	5
P-2: Requests for Society Records	9
P-3: Requests for Member Information.....	11
P-4: Requests for General Information	13
P-5: Information Incident Management.....	15

PURPOSE OF THESE POLICIES

The goal of this document is to establish the Simon Fraser Student Society's commitment to collect, use, disclose, ensure accuracy of, protect, and retain any and all personal information under control of the Society in the manner established by the *Personal Information Protection Act*.

Commented [SA1]: Purpose is to also highlight how the SFSS gathers, uses, discloses and manages privacy information of SFU students, SFSS staff and Board members. This policy strives to ensure that personal and sensitive information is handled in a way that is compliant with the PIPA. Also add that the SFSS has the authority to collect use and disclose information for the same purposes for which are reasonable, including managing employment relationships. SFSS will take reasonable security measures to protect information in it's possession

Commented [SSS2R1]: I would keep the purpose brief and high level (similar to our other policies). The rest is captured in the policy itself

Commented [SA3]: SFSS will only disclose information if there is an obligation (as per the collective agreement, under PIPA or legal obligation)

Commented [SSS4R3]: Again, will be in policy

Commented [SA5]: Include notice about random audits to determine compliance or for investigation purposes

Commented [SSS6R5]: This would be in the SOPs

POLICY REVIEW AND APPROVAL PROCESS

Each policy will be reviewed annually by any staff involved in achieving the stated policy outcome. The Policy, Research, Community Affairs Coordinator or designate will provide staff with an annual review schedule.

Where no change is required, the Board President and Executive Director (ED) or designate shall sign the policy indicating it has been reviewed.

Where a need or an opportunity for improvement arises, policy shall be created, changed, or repealed in the following way:

1. The office responsible for the policy outcome shall propose amendments and communicate those to the ED or designate.
2. The ED or designate shall review the proposed changes with the Privacy Officer and Manager – Administrative Services or designate involved.
3. Any new, amended, or repealed policy shall be signed by the ED and the Board President or designate and shared with staff and membership. |

Commented [SA7]: Add that the new policy will be shared with the staff



P-1: PERSONAL INFORMATION AND PRIVACY POLICY

<i>POLICY TYPE: PRIVACY AND INFORMATION MANAGEMENT POLICY</i>		
<i>POLICY TITLE: PERSONAL INFORMATION AND PRIVACY POLICY</i>		
<i>POLICY REFERENCE NUMBER: P-1</i>		
<i>Adopted: June 1, 2020</i>		
<i>Previous Revisions: April 3, 2017</i>		
Position	Signature	Date
Executive Director		

Policy

This policy aims to establish the standards according to which all SFSS processes will collect, use, disclose, ensure accuracy of, protect, and retain personal information, ensuring thereby that all obligations under British Columbia’s *Personal Information Protection Act* (PIPA), and Canada’s *Personal Information Protection and Electronic Documents Act* (PIPEDA) only if personal information crosses provincial or national borders, are respected.

The Policy, Research, Community Affairs Coordinator serves as the Privacy Officer of the Simon Fraser Student Society (SFSS).

Definitions

1. ‘Personal information’ means information about an identifiable individual which includes, but is not limited to names, home addresses and telephone numbers, age, sex, gender identity, marital or family status, SIN, identifying number, race, national or ethnic origin, colour, religious or political beliefs or associations, educational history, medical history, disabilities, blood type, employment history, financial history, criminal history, anyone else's opinions about an individual, an individual's personal views or opinions, and name, address and phone number of parent, guardian, spouse or next of kin. Personal information includes employee personal information but does not include workplace contact information or work product information.
2. ‘Work production information’ means information prepared or collected by an individual or group of individuals as a part of the individual's or group's responsibilities or activities related to the individual's or group's employment or business but does not include personal information about an individual who did

Commented [SA8]: This should include information verbally collected as well as email/instant message communications

Commented [SA9]: SIN

Commented [SA10]: workplace contact information

not prepare or collect the personal information. Work product information may be written or verbal information.

- 3. 'Privacy Officer' means the individual designated responsibility for ensuring that the SFSS complies with this policy and with the obligations of PIPA.

Commented [SA11]: and adheres to PIPA

Standards

- 4. The Society will ensure that:
 - a. the purpose for the collection, use, and disclosure of any personal information is clear or evident,
 - b. the process for obtaining consent for the collection, use, and disclosure of personal information is clear or evident,
 - c. the collection, use, and disclosure is limited to what is necessary for the conduct of its operations and to establish and manage employee relationships,
 - d. clients reserve the right to maintain access to and request the correction of their personal information,
 - e. the personal information it collects is accurate,
 - f. the personal information it collects is protected,
 - g. the personal information it collects is retained in a manner consistent with applicable regulations,
 - h. there are clear schedules for the retention and destruction of the personal information it possesses,
 - i. Directors, staff, and volunteers are trained so as to ensure they comply with the requirements of this policy,
 - j. annual privacy audits of Society will be conducted,
 - k. there are procedures for the prevention, reporting, containment, remediation and notification of an information incident, and
 - l. complaints, inquiries, or requests for the access to, correction of and/or removal of personal information

Commented [SA12]: establish and management employment relationships

Commented [SA13]: and to manage employee relationships

Commented [SA14]: Maybe add: obligation to a privacy breach?

Purpose of collection

- 5. Personal information will only be collected, used, or disclosed where required by the provision of Society services or programming, or the Society's adherence to its legal obligations.

Commented [SSS15]: This could be deemed implicit, as information is given to SFU who would obtain consent, then passed to us

Process for obtaining consent

- 6. The Society will obtain consent to collect, use, or disclose personal information at the time of collection, except for the purposes of, for instance:
 - a. acquiring the SFSS member registry, and
 - b. improving Society programs and services.
- 7. Subject to certain exceptions (e.g. the personal information is necessary to providing a service or product, or the withdrawal of consent would frustrate the performance of a legal obligation), clients can withhold or withdraw their consent.

Commented [SSS16]: Not sure the intention of this - I've left it simply because I assume there is a reason it is there. I don't like the idea of obtaining information without consent however, so I'm open to removing the reference here and in 6.

Commented [SA17]: Should also include proving personal information where required by law

Commented [SA18]: Consent is implied unless they opt out?

Commented [SSS19R18]: This is an interesting point. Currently I receive a list from SFU with ALL undergrad student's PI. They can unsubscribe from emails from us

Limitations on collection, use, and disclosure

- 8. The Society will only collect, use, or disclose personal information where necessary to fulfill the purposes identified at the time of collection or for a purpose reasonably related to those purposes such as the conduct of surveys intended to enhance the provision of our programs and services.

Access to personal information and requests for correction and removal of personal information

- 9. Clients have the right to access and request to correct and remove their personal information.
- 10. A request to access personal information must be made in writing and provide sufficient detail to identify the personal information being sought.
- 11. A request to correct or remove personal information must be made in writing and provide sufficient detail to identify the personal information being sought.
- 12. A minimal fee of no more than one dollar may be charged for providing access to personal information.
- 13. The Society will respond to requests from clients no later than 30 days after the client's request, unless:
 - a. the request is not detailed enough to identify the personal information requested,
 - b. a large amount of personal information is requested or must be searched and meeting the time limit would unreasonably interfere with the operations of the Society, or
 - c. more time is needed for the Society to consult with another organisation or public body to decide whether or not to provide the client access to the requested document or information.
- 14. If a request is refused in full or in part, we will provide the reasons for refusal and the recourse available to the client. Requests may be denied if they reveal personal information about another individual, threaten the safety and/or health of another individual, or reveal third party information without their consent, among other things.

Assurances of accuracy

- 15. The Society will make every reasonable effort to ensure that the personal information it uses is accurate and complete. Upon request by an individual to whom information relates, the Society will correct or annotate the information with a correction when documentary evidence, satisfactory to the Society, is provided to substantiate the correction.

Commented [SA20]: Add that requests will be responded to within 30 business days

Commented [SA21]: Provided that it has reasonable basis (for requests of information other than your own)

Commented [SSS22R21]: This policy is just referring to collection of your own PI. P3 talks about member information - although this policy is not particularly detailed, I'd prefer to keep that detail in the internal SOPs

Commented [SA23]: Also add that requests may be denied if they reveal personal information about someone else, threaten safety/health of another individual and reveal third party identity without their consent

Commented [SSS24R23]: I think we could take reasonable steps. The less we add in, the

Commented [SA25]: Duplicate as point 9

Commented [SSS26R25]: This one refers to correct or remove PI, not just access (separate in PIPA)

Commented [SSS27]: Of no more than one dollar

Commented [SA28]: requestor

Assurances of protection

- 16. The Society will protect personal information by making reasonable security arrangements to prevent the risk of unauthorized collection, access, use, disclosure or disposal of personal information.

Assurances of retention

- 17. The Society will retain personal information for a period of at least one year.

Schedule for retention and destruction of personal information

- 18. The schedule for retention and destruction of any and all personal information in the control of the Society will be outlined in SFSS Personnel Policies.

Training for Directors, staff and volunteers

- 19. The Society will provide training to Directors, staff and volunteers upon hire on the SFSS Privacy and Information Management Policies. New Directors, staff and volunteers are required to provide their signature indicating they have completed the aforementioned training during orientation. Current Directors, staff and volunteers are required to provide their signature upon completion of the aforementioned training.

Privacy audits

- 20. Annual privacy audits of Society operations will be conducted by the Privacy Officer to ensure that staff are compliant with Society policies and procedures, and that there is continuous improvement in privacy and information management practices.

Information incident

- 21. The Society will establish an information incident procedure, which will include steps on preventing (including risk identification), reporting, containing, remediating, and notifying those affected of an information incident.

Complaints, inquiries or requests

- 22. Complaints, inquiries, or requests for the access to, correction of and/or removal of personal information should be directed, in writing, to the Campaigns, Research and Policy Coordinator, who is the Privacy Officer of the Society. If the Privacy Officer is unable to resolve the concern, the Information and Privacy Commissioner of British Columbia may be contacted. The Privacy Officer may be contacted by email at policyresearch@sfss.ca.

Commented [SA29]: this includes sign off on the confidentiality policy

Commented [SSS30R29]: Sounds good. Is this for legal purposes? I won't include in the policy if it's not needed.



P-2: REQUESTS FOR SOCIETY RECORDS

<i>POLICY TYPE: PRIVACY AND INFORMATION MANAGEMENT POLICY</i>		
<i>POLICY TITLE: REQUESTS FOR SOCIETY RECORDS</i>		
<i>POLICY REFERENCE NUMBER: P-2</i>		
<i>Adopted: June 1, 2020</i> <i>Previous Revisions</i>		
Position	Signature	Date
Executive Director		

Policy

The Privacy Officer is responsible for administering all requests for Society records from members.

The ED is responsible for administering all requests for information from the public.

Clients

- Members
- Public

Definitions

- 'Society records' refers to a record the Society is required to keep as per section 20 of the Societies Act.

Process

- Where a client wishes to request Society records not available on the Society website, that client must submit a Society Record Request Form.
- Where the client is a member, the Privacy Officer will:
 - consult with the client for additional details where required,
 - collect the documents requested, ensuring no sensitive information or personal information is included in the package,
 - coordinate the time and place where the client may access and review the requested documents in accordance with Society by-laws or, where

Commented [SS31]: Previously said Admin Supervisor, but as per PIPA, this must be done by the Privacy Officer which is currently the CRPC

Commented [SA32R31]: Lets keep CRPC as privacy officer

Commented [SA33]: What does the societies act say about this? How long are we supposed to keep the minutes etc for?

Commented [SS34]: This isn't shared with members - how are they expected to use it?

Commented [SA35R34]: We should post on our webpage and mention in our Clubs newsletters maybe?

Commented [SS36R34]: Good idea - I'll ask Sindhu if it's possible to add to our "Documents" tab on the website. Unless we decide to move this policy

- appropriate, provide the client with the documents in electronic format, and
 - d. retrieve the documents after the client is finished their review where those documents are made available on location.
4. Where the client is external to the Society, the ED will:
- e. consult with the Board where appropriate,
 - f. refer the request to the Privacy Officer with direction on how to proceed.

Commented [SA37]: Are we able to add something regarding retention of records for staff/board/minutes etc? Or maybe we should have a separate policy for record retention as required by each Act where we specify time frames, the accountable parties and proper destruction of the record.

Commented [SSS38R37]: Our by-laws have provisions for "documents of the Society" which refer to records required by the Societies Act. We also have a records retention policy in our Personnel Policies that aligns with PIPA and Societies Act. I wouldn't make anything else available to students through a request for information. I think this policy in particular would fit better with the records retention policy however, and just mention privacy.



P-3: REQUESTS FOR MEMBER INFORMATION

<i>POLICY TYPE: PRIVACY AND INFORMATION MANAGEMENT POLICY</i>		
<i>POLICY TITLE: REQUESTS FOR MEMBER INFORMATION</i>		
<i>POLICY REFERENCE NUMBER: P-3</i>		
<i>Adopted: June 1, 2020</i>		
<i>Previous Revisions: April 3, 2017</i>		
Position	Signature	Date
Executive Director		

Policy

The Privacy Officer is responsible for administering all requests for member information from Directors, staff, and members.

The ED is responsible for administering all requests for information from the public.

Standards

1. Requests for member information may only be made in accordance with the standards contained in P-1: Personal Information and Privacy Policy.
2. Requests for member information regarding an individual other than one's self will be denied unless the requestor has express written permission from the individual of who the personal information pertains to.

Clients

1. Directors
2. Staff
3. Members
4. Public

Process

3. Where a client wishes to request personal information about a staff, Director or member of the Society, including but not limited to information regarding the membership or student status of a person, they must complete a Member Information Work Order.
4. Where the client is a Director or staff person, the Privacy Officer will:
 - a. consult with the client for additional details where required,

Commented [SA39]: We should think about what happened at the AGM this year and info was requested for Martin

Commented [SA40]: Where would you find this? I've never even heard of it!

Commented [SSS41R40]: This would be the work order available at the Student Centre that goes to me (in my email signature). We could harmonize this with the above work order however (unless we move that one back into Personnel Policies, then we can have one form for any privacy/records feedback or requests a la P1 #18).

- b. collect the documents requested, ensuring no sensitive information is included in the package,
 - c. coordinate the time and place where the client may access and review the requested documents or, where appropriate, provide the client with the documents in electronic format, and
 - d. retrieve the documents after the client is finished their review where those documents are made available on location.
5. Where the client is external to the Society, the ED will:
- a. consult with the Board where appropriate,
 - b. refer the request to the Privacy Officer with direction on how to proceed.

|

|

|

Commented [SA42]: We may need to add a policy on employee monitoring when we move to the new SUB because we will have card readers which may be considered as employee monitoring. So lets protect ourselves. This policy would aim to provide notice to the employees that the information of when they scan their mesh card may be collected and stored (I presume by SFU but I will confirm). The purpose of the key cards is only to provide access to

Commented [SA43]: Also have a policy on social media/technology use - would incorporate inappropriate social media posts, bullying and harassment of coworkers?

|

|

Commented [SSS44R43]: This (and the idea above) are great. I suggest these are created under our personnel policies. We have a bullying/harassment policy for staff in there currently



P-4: REQUESTS FOR GENERAL INFORMATION

<i>POLICY TYPE: PRIVACY AND INFORMATION MANAGEMENT POLICY</i>		
<i>POLICY TITLE: REQUESTS FOR GENERAL INFORMATION</i>		
<i>POLICY REFERENCE NUMBER: P-4</i>		
		<i>Adopted: June 1, 2020</i>
		<i>Previous Revisions: April 3, 2017</i>
Position	Signature	Date
Executive Director		

Commented [SS45]: State that requests will be dealt with by the Member Services Coordinators/Assistants/General Manager/Communications Coordinator and if there is PI it will be directed to the Privacy Officer. Consider changing the name of this whole document to "Privacy and Information Management Policies"

Policy

The Communications Coordinator is responsible for administering all requests for general information from Directors, staff and members.

Commented [SA46]: The new name will be the General Office

The Manager Administrative Services is responsible for administering all requests for information from the public.

Standards

1. Requests for general information will be received and handled by the Communications Coordinator and forwarded to the appropriate staff person if necessary.
2. The Privacy Officer will handle any requests for information that concern member, staff or Director privacy and personal information in accordance with the standards contained in P-1: Personal Information and Privacy Policy.

Clients

1. Members
2. Public

Process

3. Where a client wishes to request general information about the Society that is not otherwise regarding a Society record or the personal information of a staff, Director, or member of the Society, they must complete a Feedback Form.
4. Where the client is a member, the Communications Coordinator will:
 - a) consult with the client for additional details where required,
 - b) forward the request to the most appropriate staff member,

- c) provide the information requested, ensuring no sensitive information is included,
 - i. if a document is requested, collect the document requested, ensuring no sensitive information is included in the package,
 - ii. coordinate the time and place where the client may access and review the requested documents or, where appropriate, provide the client with the documents in electronic format, and
 - iii. retrieve the documents after the client is finished their review where those documents are made available on location.
- 5. Where the client is external to the Society, the ED will:
 - a. consult with the Board where appropriate,
 - b. refer the request to the Privacy Officer with direction on how to proceed.



P-5: INFORMATION INCIDENT MANAGEMENT

<i>POLICY TYPE: PRIVACY AND INFORMATION MANAGEMENT POLICY</i>		
<i>POLICY TITLE: INFORMATION INCIDENT MANAGEMENT</i>		
<i>POLICY REFERENCE NUMBER: P-5</i>		
<i>Adopted: June 1, 2020 Previous Revisions</i>		
Position	Signature	Date
Executive Director		

Policy

This policy will establish a process for managing information incidents. The Privacy Officer is responsible for the administration of this policy.

Definitions

Information incidents are when unwanted or unexpected events threaten privacy or information security. They can be accidental or deliberate and include the theft, loss, alteration, or destruction of information. An information incident may also be referred to as a privacy breach.

Commented [SA47]: We can think more about what happened with our email outage

Standards

1. The Society will ensure that:
 - a. privacy breaches are prevented through risk management procedures,
 - b. privacy breach reporting procedures are established and followed,
 - c. privacy breaches are contained as soon as reasonably possibly and efforts are made to recover any confidential or person information, and
 - d. the cause of the breach is determined, the incident is resolved, and affected parties are notified.

Prevent

2. Information incidents will be prevented through established of risk management procedures for any and all personal information in the custody of the Society.

Report

3. Staff will adhere to privacy breach reporting procedures for when and how to report privacy breaches to the Office of the Information and Privacy Commissioner (OIPC).
4. Members who have personal information in the custody of the Society may report concerns to the OIPC if they suspect a breach has occurred.

Contain

5. Privacy breaches will be contained as soon as reasonably possible and efforts will be made to recover any confidential or person information.

Remediate

6. The Society will work with relevant parties to determine the specific causes of the incident, resolve the incident, and if necessary, notify affected individuals.