GRADUATE STUDENT SOCIETY
UBC VANCOUVER

# GSS Privacy Policy

**Last revision:** March 2025

Last Updated March 17, 2025

**Designated Privacy Officer:**
privacyofficer@gss.ubc.ca

# 1 Personal Information Protection Policy

The Graduate Student Society of UBC Vancouver ("the GSS") is committed to meet its obligations under BC's Personal Information Protection Act "PIPA" .

The GSS has designated a Privacy Officer responsible for compliance with this Privacy Policy and PIPA, to ensure the accuracy, confidentiality, and security of personal information, as well as to allow individuals to request access to, and correction of, their personal information.

# 2 Definitions

2.1. In this Privacy Policy:

2.1.1 "**personal contact information**" includes an individual's

(a) e-mail address,
(b) phone number,
(c) mailing address,
(d) residential address or
(e) any other data that requires heightened protection under privacy laws.

2.1.2. "**personal identification information**" includes an individual's

(a) first name,
(b) last name,
(c) age,
(d) sex,
(e) marital status,
(f) employment information,
(g) income,
(h) social insurance number,
(i) demographic information or
(j) any other data that requires heightened protection under privacy laws.

2.1.3. "**sensitive personal information**" includes an individual's

(a) health information,
(b) racial or ethnic origin,
(c) religious beliefs,
(d) sexual orientation, or

(e) any other data that requires protection under privacy laws.

2.1.4. "**subsidiaries**" mean constituencies, affiliate organizations, committees, departments, services, groups, offices, programs, and businesses of the Society;

2.1.5. "**UBC-affiliated information**" includes an individual's

(a) UBC student number,
(b) campus-wide login,
(c) year of study,
(d) credits related to study, and
(e) faculty, program, or department of study.

2.1.6. "**University of British Columbia Graduate Student Society Vancouver**" means the society registered under the British Columbia *Societies Act* ("the GSS").

## 3 Purpose

3.1. The purposes of this Privacy Policy are to comply with the requirements of British Columbia's Personal Information Protection Act (PIPA) and to inform users how the GSS collects, uses, discloses, and protects personal information. This policy is designed to help users understand their rights and the measures we take to safeguard personal information in accordance with legal standards.

## 4 Scope

4.1. This Privacy Policy applies to the collection, use, disclosure, correction, and access to personal information by and in control of the GSS and its subsidiaries. Some subsidiaries may have supplementary privacy policies relating to their specific activities.

If there is a conflict or an inconsistency between this Privacy Policy and those passed by the subsidiaries, this Privacy Policy prevails to the extent of the inconsistency.

This Privacy Policy does not apply to

(a) business contact information;
(b) certain publicly available information listed in section 3(2) of PIPA; and
(c) personal information not subject to the requirements of PIPA.

## 5 Consent

Consent will be obtained on or before the collection, use and disclosure of personal information

except where PIPA authorizes otherwise.

5.1. **Notice of Collection:** Individuals will be informed of the purposes of collection, either verbally or in writing, on or before collecting their personal information. Upon request, individuals will be provided with contact information of our Privacy Officer.

5.2. **Consent Forms:** Consent may be obtained explicitly, such as orally, in writing, or electronically; or implicitly by providing the individual with a notice and a reasonable opportunity to decline.

5.3. **Withdrawal of Consent:** Subject to Section 5.4. of this Privacy Policy, an individual may withdraw consent where they provide reasonable notice. Upon receiving notice of withdrawal, the GSS will contact the individual to inform them about any prior uses of their information and to explain any further action that can be taken regarding their withdrawal.

5.3.1. Upon receiving notice of withdrawal, the GSS will stop collecting, using or disclosing the personal information, except where such collection, use or disclosure is permitted without consent under PIPA.

5.4. **Exception:** An individual cannot withdraw consent if doing so would frustrate the performance of a legal obligation of the Society.

## 6 Types of Information Collected

We may collect, use and disclose the following types of personal information, including but not limited to:

6.1. Employment-related information,
6.2. Financial information related to purchases of the Society's services and products,
6.3. Information obtained through Society-initiated surveys,
6.4. Information provided for Society-sanctioned services or events,
6.5. Memberships in the Society's clubs, affiliate organizations, or subsidiaries,
6.6. Personal contact information,
6.7. Personal identification information,
6.8. Sensitive personal information, and,
6.9. UBC-affiliated information.

## 7 Purpose of Collection, Use and Disclosure

7.1. The GSS will collect, use and disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances. Such purposes include, but are not limited to:

7.1.1. Authenticating identity,

7.1.2. Maintaining accurate membership records,
7.1.3. Communicating with users of the programs, services, initiatives, and products of the GSS and its subsidiaries,
7.1.4. Processing any GSS-affiliated promotions, awards, or discounts,
7.1.5. Providing, administering, and improving the services, resources, programs, events, and products of the GSS and its subsidiaries,
7.1.6. Planning, delivering, and evaluating programs, products, and services of the GSS and its subsidiaries, and in association with third parties,
7.1.7. Conducting elections, petition campaigns, and surveys,
7.1.8. Processing, documenting, and handling service issues or complaints,
7.1.9. Processing, documenting, and handling billing, payment, or reimbursement,
7.1.10. Implementing, enforcing, and monitoring compliance with the bylaws, policies, procedures, agreements, and decisions of the Society and its subsidiaries,
7.1.11. Complying with legal and regulatory requirements,
7.1.12. Protecting the GSS and its subsidiaries against fraud and error, and
7.1.13. Safeguarding the business interests of the GSS and its subsidiaries.

7.2. We will not collect, use or disclose personal information beyond what is necessary for the purposes defined in Policy Section 7.1.

## 8 Limitations

Subject to Section 5.4. of the GSS Protection of Personal Information Guidelines, the GSS will collect, use and disclose personal information about an individual only for the purposes consented to by the individual, or without consent or prior notice if permitted under PIPA.

## 9 Access to Personal Information

The GSS will provide an individual with information about its policies, practices and processes respecting personal information only upon request.

9.1. Subject to Section 9.2, upon request, the individual will be provided with:

9.1.1. Their personal information under the control of the GSS and its subsidiaries,
9.1.2. Information about the ways in which the GSS has been and are using said personal information, and
9.1.3. The names of individuals and organizations to whom their personal information has been disclosed to.

9.2. The GSS may refuse to provide an individual with their personal information where such refusal is authorized under PIPA.

9.3. Where an access to information request is refused, the GSS will:

9.3.1. Notify the individual in writing with the details of the refusal,
9.3.2. Provide the individual with the contact information of our Privacy Officer, and
9.3.3 Internally document the reason for refusal.

## 10 Accuracy and Retention of Personal Information

10.1. The GSS will make reasonable efforts to ensure that personal information collected, used, and disclosed by GSS, or on its behalf, is accurate and complete.

10.2. Subject to Section 10.3, the GSS will destroy all documents containing personal information, or the means by which such information can be associated to an individual, as soon as it is reasonable to assume that the original purpose for collecting the information is no longer being served, and the retention is no longer necessary for business or legal purposes.

10.3. Where personal information is used to make a decision that directly affects the individual, the GSS will retain that information for at least one calendar year from the date of use to ensure the individual has a reasonable opportunity to access it.

## 11 Correction of Personal Information

Upon request, the GSS will:

11.1. Correct the individual's personal information under its control, and
11.2. Send the corrected personal information to every third party to which the information was disclosed, provided that the GSS is satisfied on reasonable grounds that the correction request should be implemented.

If the GSS is not satisfied on reasonable grounds that the request should be implemented, it will annotate the personal information with the requested correction.

The GSS will make every reasonable effort to assist individuals in accessing or correcting their personal information and to respond to them as accurately and completely as reasonably possible.

## 12 Requesting Access or Correction

An individual must make a written request, consistent with the GSS's request procedures, to access or correct their personal information. The written request must include:

12.1. The individual's contact information, and
12.2. Sufficient detail to identify the personal information or correction being sought.

Requests for access or correction are generally fulfilled within 30 days of receiving it. A written notice will be provided where additional time is required.

Where the GSS is unable to provide the requested personal information, the individual will be provided with alternative approaches/suggestions to obtain and examine such information.

## 13 Third Parties

We may share personal information with third parties for the purposes outlined in the Policy.

Personal information may be processed and stored in foreign jurisdictions with different privacy laws, and the government or regulatory agencies in those jurisdictions may be able to obtain disclosure of that personal information.

When disclosing personal information to third parties, The GSS will take reasonable measures, through contractual or other means, to ensure that:

13.1. A comparable level of protection is implemented by such parties, and
13.2. the personal information is returned or destroyed once the purpose for which it was provided has been fulfilled.

## 14 Protection of Personal Information

Upon consideration of the volume and sensitivity of the personal information, The GSS will implement reasonable physical, organizational, and technological safeguards to secure the personal information against loss, theft and unauthorized access, disclosure, copying, use, modification or similar risks.

In the event of a privacy breach, the GSS will take reasonable measures for the protection of personal information and will notify the affected individuals of the breach within a reasonable time.

## 15 Complaints

Where requested by an individual, the GSS will provide them with its complaints procedure. All inquiries, questions, and complaints regarding personal information should be directed to the Privacy Officer.

## 16 For more information

For more information, to request access to personal information, or to file a complaint, please contact the GSS Privacy Officer at ppa@gss.ubc.ca.

GRADUATE STUDENT SOCIETY
UBC VANCOUVER

# Appendix I.
# Personal Information Complaints

| | |
|---|---|
| **Your name** (Last, First): | |
| **Your address:** | |
| **Your e-mail:** | **Your phone number:** |

**Nature of Complaint**

- Fee levied is inappropriate
- A time extension taken to respond to my access request is inappropriate
- No response received and no extension has been taken
- Extension has expired and no response received
- Explanation for withholding information is insufficient
- Inappropriate collection of my personal information
- Inappropriate use of my personal information
- Inappropriate disclosure of my personal information
- My personal information has not been adequately protected
- My correction request was refused without justification
- GSS did not respond openly, accurately and without delay
- Search for records not adequate

**Provide the specifics/ details of your complaint below.**

**What resolution/remedy are you seeking?**

| | |
|---|---|
| **Your Signature:** | **Today's Date:** |

GRADUATE STUDENT SOCIETY
UBC VANCOUVER

# Appendix I.
# Personal Information Complaints

***Instructions:*** *Attach a letter if there is not enough room on this form. Return the completed form to [email of privacy officer].*

GRADUATE STUDENT SOCIETY
UBC VANCOUVER

## Appendix II.
## REQUEST TO ACCESS PERSONAL INFORMATION and/or REQUEST TO CORRECT PERSONAL INFORMATION

| | |
|---|---|
| **Your name** (Last, First): | |
| **Your address:** | |
| **Your e-mail:** | **Your phone number:** |
| **Access Request:** *Please provide details of the requested personal information.* | |
| **Correction Request:** *Please provide details of the information to be corrected, and details as to why you think there are errors or omissions concerning your personal information.* | |
| **Your Signature:** | **Today's Date:** |

***Instructions:***

- *Be specific about the type of personal information you are seeking access or correction for.*
- *Attach a letter if there is not enough room on this form.*
- *Return the completed form to [email of privacy officer].*

GRADUATE STUDENT SOCIETY
UBC VANCOUVER

# GSS Protection of Personal Information Guideline

A Guide on the Implementation of the GSS Privacy Policy

Internal Document

Designated Privacy Officer
privacyofficer@gss.ubc.ca

Prepared By

Alireza Kamyabi (GSS Vice-President External Relations, 2020–2021)
Jiwan Sangha (GSS Privacy Policy Assistant, 2020–2021)

1. Modification ..... 2
2. For Clarity ..... 2
3. Scope ..... 3
4. General ..... 3
Example 1. Journalistic Purpose ..... 3
Example 2. Application of FIPPA ..... 3
5. Consent Must be Obtained ..... 3
5.1 General Principles ..... 3
Example 3. GSS Access to Member Personal Information Memorandum of Understanding ..... 4
Example 4. Collection, Use, Disclosure ..... 4
5.2 Types of Consent ..... 5
(a) Express Consent ..... 5
Example 5. Oral vs Written Consent ..... 5
(b) Implicit Consent ..... 5
Example 6. Implicit Consent ..... 5
(c) Opt-Out Consent ..... 5
5.3 Withdrawing Consent ..... 6
Example 7. Withdrawing Consent ..... 6
5.4 Where Consent Is Not Required [ss 12, 15 & 19] ..... 6
6 Collection of Personal Information ..... 7
6.1 General Principles ..... 7
6.2 Requirements Prior to Collection ..... 7
Example 8. Limitation on Councillor Information Collection ..... 7
Example 9. Purpose of Collection ..... 7
Example 10. Limitation on Event Information Collection ..... 7
Example 11. Sensitivity of Personal Information ..... 8
Example 12. Harms of a privacy breach ..... 8
7. Use of Personal Information ..... 8
7.1 General Principles ..... 8
7.2 Requirements Prior to Use of Personal Information ..... 9
Example 13. Limitation on Use ..... 9
8. Disclosure of Personal Information ..... 9
8.1 General Principles ..... 9
Example 14. Disclosing Personal Information via E-mail ..... 9
Example 15. Disclosure of Reimbursements ..... 9
Example 16. Disclosure to House Finance Committee ..... 9
8.2 Requirements Prior to Disclosure of Personal Information ..... 10
8.3 Collection, Use, Disclosure: External Organizations ..... 10
8.4 Disclosure for research or statistical purposes (without Consent) [s 21] ..... 10
9. Access to Personal Information by Individuals ..... 10
9.1 General Principles ..... 10
9.2 Requirements for Access to Personal Information ..... 10
Example 17. 'Access to Information Time Extension' E-mail Template ..... 11
9.3 Response to Access Requests ..... 11

(a) Duty to Assist ..... 11
Example 18. Duty to Assist ..... 11
(b) Contents of Response ..... 11
(c) Charging a Fee if Access Provided ..... 12
Example 19. 'Contents of Response to Access' E-mail Template ..... 12
(d) Refusal to Access ..... 12
Example 20. 'Refusal to Access' E-mail Template ..... 12
(e) Providing Access ..... 13
Example 21. 'Providing Access' E-mail Template ..... 14
**10. Correction of Personal Information ..... 14**
**10.1 General Principles ..... 14**
**10.2 Requirements Prior to Correction of Personal Information ..... 14**
**10.3 Decision Regarding Collection of Personal Information ..... 14**
**11. Personal Information Safeguards ..... 14**
**11.1 Retention of Personal Information ..... 15**
Example 22. Event Information Retention Policies ..... 15
Example 23. Councillor Information Retention Policies ..... 15
Example 24. GSS Advocates E-mail Retention Policies ..... 15
Example 25. Destruction Protocols ..... 15
**11.2 Accuracy ..... 16**
**11.3 Protection ..... 16**
(a) General ..... 16
Example 26. Safeguards Depending on Sensitivity of Personal Information ..... 16
(b) Physical Safeguards ..... 17
Example 27. Physical Safeguards of Councillor Information ..... 17
(c) Administrative Safeguards ..... 17
Example 28. Microsoft Teams Access Safeguards ..... 18
Example 29. Councillor Confidentiality Agreements ..... 18
(d) Technical Safeguards ..... 18
Example 30. Microsoft Teams Storage & Transmission Safeguards ..... 18
(e) Computers ..... 19
(f) E-mails ..... 19
(g) Meetings ..... 19
Example 31. Meeting Protocols ..... 20
**12. Privacy Breach Protocol ..... 20**
**13. Privacy Complaints Process ..... 21**
Example 32. Handling Complaints ..... 21
**14. Protection of Employees ..... 21**
**15. GSS Privacy Officer ..... 21**

## 1. Modification

This document may not be amended or changed materially without the approval of the UBC Graduate Student Society Council.

## 2. For Clarity

2.1 This document may be cited as the GSS Protection of Personal Information Guideline ("PPIG").
2.2 References in square brackets, i.e. "[s … ]" are made to the BC *Personal Information Protection Act*.
2.3 "GSS employees" includes all the Society's staff, executives, and councillors [s 1].

2.4 This guideline is complemented by the Society's Privacy Policy and Privacy Charts.

## 3. Scope

This document contains internal guidelines for the purpose of assisting the UBC Graduate Student Society ("the Society") meet its obligations to protect personal information in its custody and control in accordance with BC's *Personal Information Protection Act.*

## 4. General

4.1 Collection, use, and disclosure of personal information must only be for a reasonable purpose. What is reasonable will depend on factors such as the type or amount of personal information the Society collects, how it plans to use that information, and where or to whom (both internally and externally) it discloses that information to [s. 4].

4.2 PIPA is inapplicable in the following instances [s 3]:

(a) collection, use or disclosure is for artistic or literary purposes
(b) collection, use or disclosure is for journalistic purposes
(c) where collection, use or disclosure of personal information falls under the *Freedom of Information and Protection of Privacy Act* (FIPPA)
(d) personal information in court-related documents
(e) personal information in a note, communication, or draft decision of the decision maker in an administrative proceeding;
(f) collection/use/disclosure of the Society's employee information as long as the collection is reasonable for the purposes of establishing, managing, or terminating an employment relationship between the Society and the individual [ss 13, 15, 19]

> Example 1. Journalistic Purpose
> A purpose is journalistic where it
> (1) has a purpose is to inform the community on issues the community values,
> (2) involves an element of original production and
> (3) involves a self-conscious discipline calculated to provide an accurate and fair description of facts, opinion, and debate at play within a situation

> Example 2. Application of FIPPA
> FIPPA applies to personal information that is collected, used, or disclosed by government institutions, such as UBC. It does not apply to the GSS as a registered Society.

## 5. Consent Must be Obtained

### 5.1 General Principles

(a) The Society must obtain consent from an individual before it can:
  i. collect their personal information from the individual or a source other than the individual,
  ii. use an individual's personal information, or
  iii. disclose an individual's personal information.
(b) The Society must maintain an accurate and up to date record of the personal information it stores of an individual. This recordkeeping may be done through an active log on Excel stored in Microsoft Teams.
(c) The Society must obtain consent before or at the time it collects personal information.
(d) The Society can only require an individual to consent to the collection, use or disclosure of personal information if that information is necessary to provide a product or service of the Society [s 7(2)].
(e) Consent is not required in instances where PIPA does not apply, as outlined in Section 4.2 of this Guideline.

(f) Consent is also not required in the following cases:

i. The use or disclosure of graduate student personal information obtained through the GSS Access to Member Personal Information Memorandum of Understanding (MOU) if the use or disclosure is compliant with the MOU.

a. See section 8.3 of this Guideline for further details.

ii. Where an individual joins a Society-affiliated committee, club, or other initiative and provides their personal information voluntarily, the implicit consent principle in 5.2(b) may apply. If the requirements of 5.2(b) are not met, express consent will be required.

**Example 3. GSS Access to Member Personal Information Memorandum of Understanding**

Ordinary member information obtained from the GSS-UBC Memorandum of Understanding must be used, stored, and disclosed in a manner consistent with the terms of the MOU. For clarity, some of the terms are outlined below.

1. Purpose:
    a. communicating between the Society and its members, and
    b. verifying eligibility of students for Society-sanctioned services and programs.
2. Examples of communication
    a. Information about upcoming Society elections and referenda
    b. Information about time-sensitive emergency issues
    c. Information welcoming students to UBC and the Society
    d. Information regarding the Society's student surveys
    e. Pertinent information as deemed by the Society, e.g., the Society's newsletter
3. The Society cannot use personal information to distribute
    a. Information that discloses personal information about an individual without their consent or violates privacy or other laws
    b. Pirated software, destructive software, pornographic materials, libelous statements or any other information that may injure someone or lead to a lawsuit or criminal charges
    c. Advertisements for commercial enterprises (except Society-owned businesses)
    d. Repetitious or redundant information, or any information that is wasteful/monopolizing of resources
    e. Information that assumes another person/organization identity or role through deception or without authorization.

**Example 4. Collection, Use, Disclosure**

1. Collection of personal information includes
    a. collecting councillor or committee person information for membership
    b. collecting information from event attendees, including taking pictures at events
    c. collecting a complainant's information to process a complaint
2. Use means to view or handle personal information without disclosing it. For example
    a. e-mailing ordinary members regarding Society orientation and the Society's newsletter
    b. e-mailing event registrants about event information or reimbursing finances to event attendees
    c. processing a complaint
3. Disclosure means releasing or making the information available to another person or organization. For example
    a. disclosing reimbursement information for approval by designated members
    b. disclosing information about the complainant & complaint with GSS employees
    c. disclosing event attendee information to EPAs

## 5.2 Types of Consent

There are three methods of obtaining consent from an individual to collect, use, or disclose their personal information. The standard form of consent is express consent unless the requirements for implicit or opt-out consent are met.

### (a) Express Consent

i. An individual clearly and explicitly consents to the collection, use, and/or disclosure of their personal information. Express consent may be written or oral.
ii. To obtain express consent, the Society must
    a. inform the individual of the purpose(s) of collection/use/disclosure, and
    b. ensure the individual willingly agrees, and
    c. obtain the individual's agreement orally or in writing.
iii. Where the Society obtains consent from an individual through a written agreement, the agreement must contain:
    a. the personal information that is to be used/disclosed,
    b. the use/disclosure being consented to by the individual and/or the entity to whom the information is to be disclosed, and
    c. the date of consent.
iv. Where consent is obtained verbally, it should be documented, indicating that the three requirements in 5.2(a)(iii) have been met.

**Example 5. Oral vs Written Consent**

When deciding whether to obtain consent orally or in writing, consider the sensitivity of the personal information and its proposed use(s) or disclosure(s). If the personal information is of high or severe sensitivity, a written agreement is required. See Example 11 on how to determine the sensitivity of personal information.

### (b) Implicit Consent

i. An individual, knowing of the purpose for the collection of their personal information, voluntarily provides that information to you.
ii. Implicit consent is an appropriate alternative to express consent where the following requirements are met:
    a. an individual volunteers the personal information, and
    b. the purpose of collection/use/disclosure is obvious to the individual, and
    c. a reasonable person would think that it was appropriate for the individual to volunteer that information in those circumstances [s 8(1)].

**Example 6. Implicit Consent**

A Society member emails the Administrative Assistant to join a committee. The information provided is voluntary. It is obvious that their name and e-mail address will be used to add them to the committee roster. It is appropriate for them to volunteer their e-mail address as a means of communication regarding committee information.

In an opposite example, if that Society member provides their residential address to the AA for the purpose of joining a committee, that information is not subject to implicit consent. This is because providing a residential address is not necessary to join a committee.

### (c) Opt-Out Consent

i. An individual provides this type of consent by not declining to provide consent.
iii. Opt-out consent is an appropriate alternative to express consent where all the following requirements are met:

a. the individual is notified that Society intends to collect, use and disclose personal information for a specific, reasonable purpose,
b. the individual is provided with the purpose for collection, use, and/or disclosure,
c. the individual is provided with a reasonable amount (typically 2 weeks) of time to decline,
d. the individual does not opt out within the time provided, and
e. personal information is classified as "low sensitivity" as outlined in Example 11 [s. 8(3)].

## 5.3 Withdrawing Consent

(a) An individual may choose to withdraw or change their consent at any time except where these actions may break a legal duty or contract between the Society and the individual [s 9]. An individual may withdraw or change their consent for certain purposes and not others.

(b) To withdraw or change consent:
   i. the individual must provide the Society with reasonable notice of at least two weeks prior to withdrawing consent, and
   ii. the withdrawal of consent must not break a legal duty or contract between the Society and the individual [s 9].

(c) Requirements for the Society
   i. Where an individual submits a request to withdraw or change their consent, the Society must inform the individual what the consequences of withdrawing or changing consent will be [s 9].

Example 7. Withdrawing Consent
Where an individual wishes to opt out of receiving Society emails, the Society must notify the individual of the likely consequences of opting out – for example, the individual may not receive Society-affiliated promotions to group classes, etc.

## 5.4 Where Consent Is Not Required [ss 12, 15 & 19]

The Society may collect, use, and/or disclose personal information without consent in the following instances:

(a) it is clearly in the interests of the individual and consent cannot be obtained in a timely way,
(b) it is necessary for the medical treatment of the individual and the individual is unable to give consent,
(c) it is collected by observation at a performance, a sports meet, or a similar event
   i. at which the individual voluntarily appears, and
   ii. that is open to the public,
(d) it is available to the public,
(e) it is necessary to determine the individual's suitability for an honour or award,
(f) it is required or authorized by law,
(g) the use is necessary to respond to an emergency that threatens the life, health or security of an individual,
(h) the disclosure is for the purpose of contacting next of kin or a friend of an injured, ill or deceased individual, or
(i) the disclosure is made on reasonable grounds to believe that compelling circumstances exist that affect the health or safety of any individual. In this case, a notice of disclosure must be mailed to the last known address of the individual to whom the personal information relates.

# 6 Collection of Personal Information

## 6.1 General Principles

(a) The Society may only collect personal information for a purpose that a reasonable person would consider appropriate in the circumstances.
(b) The collection must be limited to the amount and type of personal information that is necessary to fulfill the purposes for collecting it – broad/ overcollection is not permitted.
(c) Even if an individual volunteers more personal information than is needed for the Society's intended purposes, the Society cannot record, use or disclose the irrelevant information.

## 6.2 Requirements Prior to Collection

(a) The Society must notify individuals of the purposes for collecting personal information before or at the time of collection [s. 10(1)]. The notification should be clear, simple, and detailed. It should:
    i. provide a description of personal information to be collected in accordance with the definition of personal information outlined in Policy 18.1.1 of the GSS Policy Manual,
    ii. provide a description of the purpose of collection as outlined in Policy 18.7.2 of the GSS Policy Manual,
    iii. provide details for when/whom the Society will be sharing the information with (i.e., external organizations, if any), and
    iv. provide the contact information of the GSS Privacy Officer.

(b) When deciding whether to give notice verbally or in writing, the Society should consider the sensitivity of the personal information it is collecting and its proposed use(s) or disclosure(s).
    i. If the personal information is of high or severe sensitivity, a written notice is required.
    ii. See Example 11 on how to determine the sensitivity of personal information. Generally, the harm resulting from unauthorized access, use, or disclosure is the central consideration in determining the sensitivity of personal information. Example 12 outlines the different types of harms that the Society should consider in its assessment of the sensitivity of personal information.

**Example 10. Limitation on Event Information Collection**

When collecting information to provide a service (e.g., an event), collect only information that is necessary for the event. Standard information for a Society -sponsored event includes the individual's name, phone number, e-mail, and student number.

Collecting other personal information such as an individual's residential address is prohibited in instances where it is not necessary. An individual's residential address for a specific event may be necessary. For example, a residential address may be necessary where supplies need to be sent to an individual for participation in the event.

**Example 8. Limitation on Councillor Information Collection**

Where a Councillor completes a "Declaration of Election to the GSS Council" form, the Society should not ask for a copy of their proof of enrolment unless deemed necessary. The Councillor's acknowledgement that they are a graduate student will suffice.

**Example 9. Purpose of Collection**

1. To verify graduate student identity for AGM, events, or other student-specific initiatives
2. To verify that a councillor is a graduate student prior to election
3. To administer the Society's events
4. To reimburse members for paid event attendance
5. To process or respond to complaints

**Example 11. Sensitivity of Personal Information**[1]

| Sensitivity | Definition | Classification | Examples[2] |
|---|---|---|---|
| Low | Information or data that, if used, disclosed, or accessed without proper authorization, will not result in harm or negative impacts for those affected. | Public | • Names and work contact information<br>• Information that is posted on the Society's public website |
| Moderate | Information or data that, if used, disclosed, or accessed without proper authorization, are likely to cause minor harm or negative impacts and/or be disadvantageous for those affected. | Restricted | • Membership in Committee<br>• Salary information<br>• Non-identifiable personal information |
| High | Information or data that, if used, disclosed, or accessed without proper authorization, are likely to cause serious harm or negative impacts for those affected. | Confidential | • Information from UBC MOU<br>• Student name, number, e-mail, address<br>• Email communications<br>• Residential address |
| Severe | Information or data that, if used, disclosed, or accessed without proper authorization, are likely to cause severe harm or negative impacts and/or damage to those affected. | Strictly Confidential | • Employee SIN<br>• Date of birth<br>• Official government documents<br>• Bank account information<br>• Credit card information<br>• E-mail communications related to the GSS Advocates service<br>• Information relating to Graduate Student Financial Aid (GSFA)<br>• Information relating to complaints |

Example 12. Harms of a privacy breach[3]

1. loss of privacy;
2. breach of confidentiality;
3. loss of data and information integrity;
4. loss of information value;
5. financial impacts;
6. personal injury;
7. loss of life;
8. harm to business relationships; and
9. reputational damage.

# 7. Use of Personal Information

## 7.1 General Principles

(a) Use means to view or handle personal information within the Society without disclosing it.
(b) There are limitations to the use of personal information.
    i. The use of personal information must be consented to by the individual.
    ii. The Society may only use personal information for a reasonable purpose.

iii. The use of personal information must also be limited to the amount and type of personal information that is necessary to fulfill the purpose(s) of collection.

### 7.2 Requirements Prior to Use of Personal Information

(a) Consent for use must be obtained before or at the time of the use of personal information.
(b) The Society must provide an individual with a clear description of how the personal information will be used.
(c) The Society must obtain consent again from an individual if their personal information is to be used for a different purpose than what was originally consented to.

Example 13. Limitation on Use

1. If the Society collects a student's study status for a specific AMS/GSS subsidy, it cannot use that information to determine whether that individual should be eligible for a different subsidy.
2. If the Society collects personal information for event sign-ups, it cannot use the information to send monthly newsletters to the individual without their consent.

## 8. Disclosure of Personal Information

### 8.1 General Principles

(a) Disclosure means releasing or making the information available to another person or organization, both internally and externally.
(b) There are limitations to the disclosure of personal information.
    i. The disclosure of personal information must be consented to by the individual.
    i. The Society may only disclose personal information for a reasonable purpose.
    ii. The disclosure of personal information must be limited to the amount and type of personal information that is necessary to fulfill the purpose(s) of collection.
(c) The disclosure should be made in a secure manner. See Example 14 for disclosure practices regarding e-mails.

Example 14. Disclosing Personal Information via E-mail

1. Do not send any personal information through non-GSS e-mail accounts.
2. Do not transmit personal information via e-mail unless necessary. You may include personal information that is classified as low or moderate sensitivity in the body of emails. The subject line of the email should include a confidentiality indicator. See Example 11 on how to determine the sensitivity of personal information.
3. If you are sending personal information classified as highly/severely sensitive over email, it is important that you first encrypt the attachment.
    a. For instructions on encryption, see: https://isit.arts.ubc.ca/send-files-securely/

Example 15. Disclosure of Reimbursements

All information regarding reimbursements to an individual must be stored on Microsoft Teams. Once a reimbursement list has been approved for processing, the list must be removed from the Microsoft Teams channel. Access to this information is no longer necessary for employees in the channel to perform their work. The list should be moved to a channel that is only accessible to the General Manager.

Example 16. Disclosure to House Finance Committee

Do not disclose personal information of members to the Committee for reimbursements/payments made to ordinary members. Only disclose monetary amounts.

### 8.2 Requirements Prior to Disclosure of Personal Information

(a) Consent for disclosure must be obtained before or at the time of the disclosure of personal information.
(b) The Society must provide an individual with a clear description of the purpose and method of disclosure.

### 8.3 Collection, Use, Disclosure: External Organizations

(a) The Society may disclose personal information to a third-party organization without consent of an individual if
    ii. the individual has already consented to the collection of their personal information,
    iii. the personal information is disclosed to the third-party solely for the purposes for which the information was previously collected, and
    iv. the personal information is required to assist the third-party to carry out work on behalf of the Society [s 18(2)].
(b) The disclosure must be consistent with Policy 18.13 of the GSS Policy Manual.

### 8.4 Disclosure for research or statistical purposes (without Consent) [s 21]

The Society may disclose, without the consent of the individual, personal information for a research purpose, including statistical research, only if

(a) it is impracticable for the Society to seek the consent of the individual for the disclosure,
(b) the research purpose cannot be accomplished unless the personal information is provided in an individually identifiable form,
(c) the disclosure is on the condition that it will not be used to contact persons to ask them to participate in the research,
(d) linkage of the personal information to other information is not harmful to the individuals identified by the personal information and the benefits to be derived from the linkage are clearly in the public interest,
(e) the organization to which the personal information is to be disclosed has signed an agreement to comply with all the following:
    i. PIPA,
    ii. the policies and procedures relating to the confidentiality of personal information of the Society,
    iii. any additional security and confidentiality conditions imposed by the Society,
    iv. a requirement to remove or destroy individual identifiers at the earliest reasonable opportunity, and
    v. a prohibition of any subsequent use or disclosure of that personal information in individually identifiable form without the express authorization of the Society.

## 9. Access to Personal Information by Individuals

### 9.1 General Principles

(a) If the Society has personal information about an individual, the individual has the right to
    i. access their own personal information held by Society
    ii. know how Society has used or continues to use their personal information, and
    iii. know to whom and when the Society disclosed their personal information.

### 9.2 Requirements for Access to Personal Information

(a) To access their personal information, an individual
    i. must complete the “Request to Access Personal Information and/or Request to Correct Personal Information” Form, and
    ii. must provide enough information so that the Society can find the information with reasonable effort.

(b) The individual does not need to state why they are asking for the personal information.

(c) The Society must respond to all access requests within 30 days unless any of the following conditions apply:
   i. The applicant has not provided enough information to allow the Society to find the requested personal information or document.
   ii. A large amount of personal information is requested and meeting the time limit would unreasonably interfere with the Society's operations.
   iii. The Society must consult with another organization to decide if access should be given [s 31(1)].

(d) If the conditions outlined in 9.2(c) are not met, the Society may seek an extension from the BC Privacy Commissioner.

(e) If the Society extends the time limit in accordance with the conditions outlined in section 9.2(c), it must provide the applicant with
   i. why it is taking more time (reference a reason in 9.2(c)),
   ii. when it will respond to the request, and
   iii. that the applicant can complain to the BC Privacy Commissioner about the Society taking more time [s 31(2)].

Example 17. 'Access to Information Time Extension' E-mail Template

Thank-you for contacting the UBC Graduate Student Society. We write to inform you that we will need an additional [*insert time here*] to process your request because [*reference a reason in section 9.2(c) or state if you have obtained consent from the BC Privacy Commissioner for an extension*]

We will get back to your request by [*insert time here*]. Please note that you can make a complaint to the British Columbia Office of the Privacy Commissioner if you are dissatisfied with the timeline provided. The information can be found here: https://www.oipc.bc.ca/for-the-public/how-do-i-make-a-complaint/

## 9.3 Response to Access Requests

### (a) Duty to Assist in Requests

   i. The Society has a duty to assist individuals upon a request for access or correction of personal information.
   ii. The Society must
      a. make a reasonable effort to help an applicant seeking access to their personal information,
      b. respond to an applicant as accurately and completely as is reasonably possible, and
      c. unless PIPA says otherwise, provide the applicant with the personal information requested or, if the personal information cannot be reasonably provided, an opportunity to view it.

Example 18. Duty to Assist

Assistance may include providing the individual with the form, helping them complete the form, and answering any general questions. Do not provide contradictory or erroneous information – check the procedures before you provide a response.

### (b) Contents of Response

   i. In response to an access request, the Society must inform the individual, within 30 days,
      a. whether the Society has the individual's personal information,
      b. whether the Society will give the individual access to all or part of their personal information, and
      c. if access will be given, where, when and how it will be provided.

## (c) Charging a Fee if Access Provided

i. The Society may charge a minimal fee for access to personal information.
   a. If the Society provides photocopies of information, it may charge $0.10 per photocopy.
   b. It may charge labour fees for employees working on the access request (i.e., the employee's hourly rate multiplied by the time it would take for the request to be fulfilled).[4]

ii. The fee charged must solely be the cost of producing the requested personal information. This includes photocopying, printing, or other administrative costs.

iii. Where the Society will charge a fee, the Society must, prior to the service,
   a. provide the applicant a written estimate of the fee and
   b. if necessary, require the applicant to pay a deposit for all or part of the fee.

Example 19. 'Contents of Response to Access' E-mail Template

No personal information: Thank-you for contacting the UBC Graduate Student Society. We write to inform you that we are unable to fulfil your access to information request because we do not have any documents containing personal information about you.

Personal Information: Thank-you for contacting the UBC Graduate Student Society. We write to inform you that the Society is processing your request and will get back to you within 30 days. The estimated cost of the request is [*insert cost per 9.3(c)*]. Please inform us if you would like to continue with the request and accept the costs associated with processing your request.

If you choose to proceed with the request, you will be provided an [*encrypted email/photocopy/other means*] within [*insert time here – must not be longer than 30 days unless an exception applies*].

*Note: See section 9.3(e) of this Guideline for an example of how access should be provided.*

## (d) Refusal to Provide Access

i. Where the Society refuses to provide access to an individual, it must inform the individual
   a. the reasons for refusing access
      1. See Sections 9.3(c)ii and 9.3(c)iii of this Guideline for reasons for refusal. Include one of these reasons for refusal in the response.
   b. the sections of PIPA that allows or requires the Society to refuse access,
      1. Cite section 23(3) or 23(4) of BC PIPA, as applicable
   c. the contact information of the Privacy Officer, and
   d. that the applicant may ask the Commissioner to review the Society's decision to refuse access within 30 days of being notified of the refusal.

Example 20. 'Refusal to Access' E-mail Template

Thank-you for contacting the Graduate Student Society. We write to inform you that we are unable to fulfil your request for access to personal information because [*insert reason for refusal; see 9.3(c)ii and 9.3(c)iii of this Guideline for reasons for refusal*].

According to [*section 23(3) or 23(4)*] of BC *Personal Information Protection Act,* we are unable to provide you access to personal information because [*cite the specific provision in PIPA from sections 23(3) or 23(4)*]. If you have further questions, please feel free to contact the GSS Privacy Officer, [*insert GSS Privacy Officer Contact Information*].

You may also ask the BC Privacy Commissioner within 30 days of being notified of this refusal to review our decision.

ii. The Society may refuse to disclose personal information and other information where [s 23(3)]:
    a. the information is protected by solicitor-client privilege;
    b. the disclosure would reveal confidential commercial information that if disclosed, could, in the opinion of a reasonable person, harm the competitive position of the Society;
    c. the information was collected or disclosed without consent per sections 12 and 18 of PIPA, for the purposes of an investigation and the investigative proceedings and appeals have not been completed;
    d. the information was collected or created by a mediator or arbitrator in the conduct of a mediation or arbitration for which he or she was appointed to act
        1. under a collective agreement,
        2. under an enactment, or
        3. by a court.
    e. Note: If the Society can redact information referred to in a-c, the Society must provide the individual with access to the personal information after such information is redacted.

iii. The Society must not disclose personal information and other information where [s 23(4)]:
    a. the disclosure could reasonably be expected to threaten the safety or physical or mental health of an individual other than the individual who made the request;
    b. the disclosure can 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;
    c. the disclosure would reveal personal information about another individual;
    d. the disclosure would reveal the identity of an individual who has provided personal information about another individual and the provider does not consent to the disclosure of their identity
    e. Note: If the Society can redact information referred to in a-d, the Society must provide the individual with access to the personal information after such information is redacted.

## (e) Providing Access

i. The Society must only provide access to personal information to an individual once it has confirmed the identity of the individual.
ii. An individual's identity will be confirmed by assessing the accuracy of the details in the "Request to Access Personal Information and/or Request to Correct Personal Information" Form with the personal information the Society has of the individual (if any). Where no personal information is found, a request for access may be denied.
iii. Do not provide access to personal information unless you are sure of the identity of the applicant and the applicant's right of access.
iv. Where PIPA requires the Society to provide access, the Society must provide the applicant with
    a. access to their personal information,
        1. Provide the individual with the specifics of the personal information you have on them (for example: e-mail address, student number, etcetera)
    b. information on how the Society has used or is using their personal information (see Policy 18.7.2 of the GSS Policy Manual),
    c. the names of the individuals and organizations the Society has disclosed their information to, and
    d. the purpose(s) for which the Society has disclosed the individual's personal information.
v. If an applicant's personal information is in electronic form, the applicant has the option to receive a copy of the information in electronic or paper form.
    a. If you are providing personal information to an individual in electronic form, refer to section 11.3(f) of this Guideline for best practices in transferring information over e-mail.

Example 21. 'Providing Access' E-mail Template

Thank-you for contacting the UBC Graduate Student Society. You are hereby provided access to [*all or part*] of your personal information. [*If the individual is provided access to only part of the information, follow the 'Refusal to Access E-mail Template' guideline for the part of the information that is refused*].

Please find the encrypted attachment detailing the information of your request.

*Note: The following should be in an encrypted attachment. See Example 14 on instructions for encryption.*

The GSS has the following personal information about you on file [*list personal information you have on individual*]. The GSS has used this information in the following manner [*insert reason(s) per Policy 18.7.2 of the GSS Policy Manual*]. The GSS has disclosed your personal information to the following entities [*insert other organizations to whom personal information may be disclosed*]. This disclosure was made for the purpose of [*insert reason(s) per Policy 18.7.2 of the GSS Policy Manual*].

# 10. Correction of Personal Information

## 10.1 General Principles

(a) The Society is responsible for making reasonable efforts to ensure that personal information is accurate and complete, and to correct personal information if it is not.
(b) An individual who believes that there is an error or omission in their personal information can request a correction of the personal information.
(c) The Society cannot charge a fee for correction of personal information.

## 10.2 Requirements Prior to Correction of Personal Information

(a) An individual requesting correction of their personal information must
    i. Complete the "Request to Access Personal Information and/or Request to Correct Personal Information" Form, and
    ii. Provide enough background information in the Form so that the Society, with reasonable effort, can identify the correction being sought.

## 10.3 Decision Regarding Correction of Personal Information

(a) The Society must decide whether, on reasonable grounds, correction of personal information is warranted.
(b) If the correction is warranted, the Society must do the following:
    i. correct the personal information as soon as possible, and
    ii. send the corrected personal information to every organization that the Society disclosed the wrong information to during the year before the correction date.
(c) Where the Society decides not to correct the personal information, it must annotate the personal information that such a request was made. This may be done by attaching a copy of the "Request to Access Personal Information and/or Request to Correct Personal Information" Form to the personal information.

# 11. Personal Information Safeguards

PIPA requires safeguards to be implemented by the Society to protect personal information under the custody or control of the Society. PIPA requires that personal information (1) only be retained for as long as necessary (2) be accurate, and (3) be adequately protected through physical, administrative, and technical safeguards.

## 11.1 Retention of Personal Information

(a) Subject to subsection (b) of this Guideline, the Society must destroy all documents containing personal information or remove the means by which the personal information can be associated with an individual. The Society must do so as soon as it is reasonable to assume that
   i. the purpose for which that personal information was collected is no longer being served by retention of the personal information, and
   ii. retention is no longer necessary for legal or business purposes.

(b) Where the Society uses an individual's personal information to make a decision that directly affects the individual, the Society must retain that information for at least one year after using it.

(c) Personal information may need to be stored for a longer period to comply with the Society's legal or audit requirements.

Example 22. Event Information Retention Protocol

Where an event has been completed, the attendance sheet should be discarded. It should not be saved on any platform because it is no longer necessary for the Society's purposes (unless there is financial information necessary for audits, in which case it may be kept for 7 years).

Eventbrite contains highly sensitive personal information, especially credit card information & a billing postal code for paid events. Eventbrite information on the platform must be deleted 90 days following an event.

Example 23. Councillor Information Retention Protocol

Keep the Declaration of Election to the GSS Council in "active" records a year after the term in GSS DTE Server (for digital files) or in a file cabinet (physical files). Move the form to archived records after. Before moving the form, redact everything except the student's name, department, email and phone number.

Example 24. GSS Advocates E-mail Retention Protocol

The e-mails sent to the GSS Advocates e-mail address must be permanently deleted after completion of a case. All relevant case information should be uploaded on MS Teams where absolutely necessary, for a period no longer than absolutely necessary. The MS Teams Channel should only be accessible to those who require the information to complete their job duties.

All substantial advocacy emails on employee accounts must be permanently deleted from the e-mail address and uploaded on MS Teams where absolutely necessary, for a period no longer than absolutely necessary.

Example 25. Destruction Protocols

1. Society employees have a legal obligation to ensure that personal information that is no longer necessary for the Society's business or legal purposes is destroyed.
2. Any of the following are acceptable methods of destroying personal information:[5]
   a. using a software utility, such as "Secure Erase" that erases, overwrites or encrypts the data;
   b. magnetically erasing (degaussing) the data;
   c. formatting a device after encrypting; or
   d. using a machine that physically deforms or destroys the device to prevent the data from being recovered.
3. Using the "Empty Recycle Bin/Trash", "Delete", "Remove", and "Format" operating system commands are not acceptable methods for destruction.

## 11.2 Accuracy

(a) The Society must make a reasonable effort to ensure that personal information is accurate, especially where the personal information is
   i. likely to be used by the Society to make a decision that affects the individual to whom the personal information relates, or
   ii. likely to be disclosed by the Society to another organization.

## 11.3 Protection[6]

Protection of personal information includes three types of safeguards: physical, administrative, and technical. There are also technology-specific safeguards that must be implemented to ensure that personal information is protected in computers, e-mails, and meetings.

### (a) General

   i. The Society must implement protect personal information in its custody or control. The safeguards implemented for the protection of personal information must be proportional to the sensitivity of such information. See Example 26 which outlines the sensitivity of personal information and the corresponding safeguards which must be implemented for its protection.
   ii. In general, the safeguards implemented for the protection of personal information by the Society should prevent the following:
      1. someone from being able to read, use, copy or disclose personal information when they are not authorized to do such activities,
      2. someone from stealing or losing personal information, and
      3. someone from changing, destroying, or improperly disposing of personal information.

Example 26. Safeguards Depending on Sensitivity of Personal Information[7]

| Sensitivity | Definition | Safeguard | Examples[8] |
|---|---|---|---|
| Low | Information or data that, if used, disclosed, or accessed without proper authorization, will not result in harm or negative impacts for those affected. | • occasional audits<br>• regular backups to ensure availability and integrity of information | • Names and work contact information<br>• Information that is posted on the Society's public website |
| Moderate | Information or data that, if used, disclosed, or accessed without proper authorization, are likely to cause minor harm or negative impacts and/or be disadvantageous for those affected. | • periodic audits<br>• physical: secure & locked location storage<br>• digital: authorized access via password | • Membership in Committee<br>• Salary information<br>• Non-identifiable personal information |
| High | Information or data that, if used, disclosed, or accessed without proper authorization, are likely to cause serious harm or negative impacts for those affected. | • regular audits<br>• encryption if sent digitally<br>• physical: secure & locked location storage with restricted access + clean desk policy<br>• digital: authorized & authenticated access via password | • Information from UBC MOU<br>• Student name, number, e-mail, address<br>• Email communications<br>• Residential address<br>• Affidavit of Election to the GSS Council |

| | | | |
|---|---|---|---|
| Severe | Information or data that, if used, disclosed, or accessed without proper authorization, are likely to cause severe harm or negative impacts and/or damage to those affected. | • frequent audits<br>• double authentication of recipient & encryption if sent digitally<br>• physical: secure & locked location with restricted access + clean desk policy + access log*<br>• digital: authorized & authenticated access via password + access log*<br><br>*Access log must include time, date, reason, and signature of access where access to the information is no longer a part of everyday work duties. | • Employee SIN<br>• Date of birth<br>• Official government documents<br>• Bank account information<br>• Credit card information<br>• E-mail communications related to the GSS Advocates service<br>• Information relating to Graduate Student Financial Aid (GSFA)<br>• Information relating to complaints |

## (b) Physical Safeguards

Physical Safeguards refer to the physical measures, policies, and procedures to protect personal information. These safeguards include facility security, physical location access controls, and workstation use and security.

All Society employees must comply with the following requirements:

i. Lock file cabinets and areas where personal information is stored.
ii. Restrict unnecessary employee access to storage areas, filing cabinets, or online platforms.
iii. Only take personal information out of secure environments if they have: official authorization from the Society's president or a person designated on their behalf, an operational need, and there are no other reasonable means to accomplish the task. Where possible, employees must take copies instead of originals of documents. When taking personal information home in electronic form, employees must ensure that the information is first encrypted.
iv. Remove files and documents containing personal information off their desk at the end of the day.
v. Shred papers containing personal information, and never place any personal information in a garbage can or recycling bin without shredding.
vi. Destroy computer hard drives that contain personal information before they are discarded.

Example 27. Physical Safeguards of Councillor Information

Information on certain forms, such as Affidavit of Election to the GSS Council, is highly sensitive personal information. If such forms are placed in a binder physically located at the Society's Office, ensure the binder is stored in a locked cabinet. For additional security safeguards, follow the procedures for high-sensitivity personal information.

## (c) Administrative Safeguards

Administrative Safeguards refer to the administrative processes, policies, and procedures to protect personal information against a privacy breach or unwanted disclosure. These safeguards include training, audits, recordkeeping, and agreements.

The Society's Privacy Officer must, alone or in combination with a designated individual, comply with the following administrative requirements:

i. Require all Society employees (especially GSS Office) to be trained and informed, once a year, of the content of these Guidelines, the Society's Privacy Policy, the Society's Privacy Charts, and the disciplinary consequences of not following them.
ii. Mandate employees to complete the UBC Privacy & Information Security Fundamentals Training.
iii. Require all employees to sign a confidentiality agreement for the protection of personal information.
iv. Implement role-based access to physical environments such as offices and filing cabinets so that personal information, especially highly and severely sensitive information, is accessible only to those employees who need such information for their duties.
v. Conduct regular privacy audits, every six months, to ensure that the Society employees are complying with the Society's privacy protocols. These audits must be logged on Microsoft Teams.
vi. Maintain an updated record of where all personal information about members may be found.

**Example 28. Microsoft Teams Access Protocol**
Do not add GSS Councillors/ Staff to Microsoft Teams channels that are not necessary to perform their work – mere convenience is *not* enough for access. Only provide access on a necessity basis. Provide only as much access as is needed for their duties.

Lock channels in Microsoft Teams and provide passwords to only those who require the information as part of their work.

**Example 29. Councillor Confidentiality Agreements**
All Councillors must sign a confidentiality agreement. Members of the AMS and Graduate Caucus must sign a confidentiality agreement immediately after election by council.

## (d) Technical Safeguards

Technical Safeguards refer to the technical measures, policies, and procedures to protect personal information. These safeguards include access controls, authentication measures, and information transmission, device, and media security.

To ensure that personal information is protected through these safeguards, all Society employees must

i. where possible, communicate passwords via phone, rather than email. This includes encryption passwords.
ii. refrain from keeping a password log unless via a designated and secure password storage software. If a password log of encryption passwords must necessarily be kept without a software, delete the log as soon as the encrypted information is no longer necessary for the Society's business or legal operations.
iii. avoid emailing or faxing personal/confidential information on a voice mail message.
iv. encrypt personal information stored on mobile electronic devices such as laptops and USB flash drives, especially where the information is highly/severely sensitive.
v. not store personal information on websites/servers hosted outside of Canada – e.g., Dropbox, Google Drives / Docs / Hangouts, Skype, Slack, Facebook.
vi. securely wipe all personal information from hard drives before discarding them. Simply deleting files off a hard drive is not enough as deleted files can be recovered. If you are unsure, the most secure method of destroying personal information is to physically destroy the hard drives.

**Example 30. Microsoft Teams Storage & Transmission**
The Society's File Sharing, Collaboration & Messaging Tools (i.e., Microsoft Teams, SharePoint) are a permitted platform to store and transmit personal information of all sensitivity.

## (e) Computers

When working on a computer within the GSS building or at home, the following protocols must be followed to ensure that personal information is protected:

i. Position computer monitors so that personal information cannot be seen by unauthorized personnel or by visitors. Enable the privacy guard feature if available.
ii. Keep personal information securely locked by using passwords to access computers. Use password-protected computer screensavers.
iii. Ensure computers and network are secure by using firewalls, intrusion detection software, antivirus software, and by encrypting personal information. Ensure all software is updated regularly.
iv. Use strong and secure passwords[9] to ensure that only authorized employees have access to computer storage devices or to the network. A strong password is one that is 16 or more characters long, and contains: no dictionary words, at least one capital letter and one number/symbol.
v. Change passwords to logins regularly.
vi. Only use the Society's provided computer unless absolutely necessary to use your own.
vii. Avoid saving personal information directly on a device. Save personal information on a secured network drive such as Microsoft Teams. Do not use cloud storage services such as Dropbox, Box, One Drive or Google Drive to store Society-related information unless approved.
viii. Where personal information must inevitably be downloaded on to a personal computer, delete Society-related documents off the device as soon as you're finished working with it, then empty the computer trash.
ix. Log out of work computer as soon as you're finished for the day.

## (f) E-mails[10]

Where Society employees work with personal information through e-mails, they must ensure that personal information is protected. In particular, they must

i. not forward emails to their personal e-mail address. Always use the e-mail address assigned by the Society for Society-related matters.
ii. only use a mobile device, such as a smartphone, to access their Society-associated email account if proper security controls are in place.
iii. not store sensitive documents on their personal phone unless absolutely necessary. If such information must be stored on their mobile device, the information must be encrypted.
iv. place all email addresses in the "Bcc" (blind carbon copy) field when sending emails to multiple personal email addresses.
v. exercise extreme caution when emailing personal information outside GSS emails. Emails sent from the Society's email accounts to external email accounts are not a confidential and secure method of communication. If a someone initiates contact with Society employees using a non-secure e-mail account (i.e., Hotmail or Google), the employee may respond to the email, but they may only discuss the individual's personal information if the individual explicitly consents for them to do so.
vi. not use their Society email account for personal communications. If they use their Society-affiliated email account for personal uses, these communications may not remain private. While the Society does not, as a routine matter, inspect personal emails stored on these accounts, the Society may need to access these emails under certain circumstances, including responding to lawful subpoenas or court orders; investigating misconduct, determining compliance with the Society's policies, and searching for electronic messages, data, files, or other records that are required for the Society's business continuity purposes.

## (g) Meetings

i. Establish exactly what will be recorded in the meeting. Establish the format, content, and level of detail of the recording. Clearly define what the record (i.e., meeting minutes) will and will not contain. Ask: which facts/information need to be documented to support the objectives of the meeting?

ii. Establish who will officially take minutes in the meeting. This individual is responsible for determining how the meeting minutes will be created, maintained, used, disclosed, and made available. Where applicable, ensure others do not maintain alternative records of the meeting.
iii. Determine, at the outset, how notes and other information, not included in the official meeting minutes record, will be treated. Inform and instruct meeting attendees of the recording and note-taking requirements at the beginning of the meeting.
iv. Determine, at the outset, how personal/confidential information will be shared, discussed and/or recorded during the meeting. Ask attendees to follow privacy/confidentiality requirements. Ensure records contain only information that can be disclosed to the public.
v. Establish guidelines for recording virtual meetings.

Example 31. Meeting Protocol

1. Save all meeting information, including meeting minutes and agendas on MS Teams.
2. All communications re: meetings should be through the Society's provided email addresses.
3. All meetings should be set up, especially if being recorded, through MS Teams.
4. Depending on the sensitivity of the personal information discussed within a meeting and the objectives of the meeting, ensure that such information is not directly recorded in the meeting minutes.
5. Refrain from recording virtual meetings, especially if they discuss personal information. Where a virtual meeting must necessarily be recorded, attendees must be notified prior to the recording of (1) the recording, (2) the purpose of the recording, (3) how long the recording will be retained for, and (4) they can object to the recording for a reasonable reason.

## 12. Privacy Breach Protocol[11]

(a) Upon a privacy breach, the Society, in particular the Privacy Officer, must
   i. Assess and document the scope of the breach, including:
      a. who had unauthorized access to personal information,
      b. what medium is involved – hard copy, electronic, verbal,
      c. which information was compromised – name, address, student number, etc.,
      d. how many were individuals affected,
      e. whether this is a one-time occurrence, potentially repeatable or an on-going problem, and
      f. the likely cause(s) or circumstance(s) of the event.
   ii. Contain the breach by immediately by
      a. making arrangements to retrieve the records,
      b. suspending the process or activity that caused the breach,
      c. taking the targeted application off-line,
      d. changing passwords, and
      e. any other actions as needed to contain the breach.

   iii. Document the incident, including
      a. date, time, location of the incident,
      b. who was affected,
      c. how the incident was discovered,
      d. when and to whom the incident was reported to, and
      e. any other relevant information (for example safeguards breached – e.g. locks, alarm system, passwords, encryption).
   iv. Investigate the breach
   v. Take action to prevent future breaches – for example, develop or change privacy policy or practices, use enhanced software, and/or provide staff training on privacy and security.
   vi. Notify affected individuals within a reasonable time, where possible. Keep a record of the notice. The notice should include
      a. a description of the incident,

b. an explanation of corrective steps taken,
c. and a protocol of how the problem will be prevented in the future.

vii. Notify the University if the information relates to the GSS-UBC MOU.[12]

## 13. Privacy Complaints Process[13]

(a) Where a privacy complaint is received informally, the Society must notify the individual about the formal complaints procedure, including a copy of the Society's Privacy Policy and the "Personal Information Complaints" Form. Do not answer complaints where a formal process is not followed.

(b) Investigate all complaints and take appropriate measures in response if a complaint is justified, including amending the Society's policies and practices if necessary.

Example 32. Complaints Processing Protocol

1. All privacy-related complaints must be handled by the Society-appointed Privacy Officer.
2. Complaints must be replied to within a reasonable time, typically of 2 weeks.
3. If it is unclear whether the individual is making a correction, access, or complaints request, clarify as it is your duty to assist. Provide the individual with all applicable forms and only respond to a complaint if the formal complaints process is followed.

## 14. Protection of Employees

The Society must not dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee of the Society, or deny that employee a benefit, because

(a) the employee, acting in good faith and on the basis of reasonable belief, has disclosed to the BC Privacy Commissioner that the Society or any other person has contravened or is about to contravene the Society's legal obligations under PIPA,

(b) the employee, acting in good faith and on the basis of reasonable belief, has done or stated an intention of doing something that is required to be done to avoid having any person contravene the Society's legal obligations under PIPA,

(c) the employee, acting in good faith and on the basis of reasonable belief, has refused to do or stated an intention of refusing to do anything that is in contravention the Society's legal obligations under PIPA, or

(d) the Society believes that an employee will do anything described in paragraphs a-c.

## 15. GSS Privacy Officer

(a) The Society must have a designated Privacy Officer at all times whose contact information must be available publicly (for example: on the GSS website), and on all privacy-related documents.

(b) The Privacy Officer must fulfil all of the Society's privacy-related obligations not limited to those outlined in these Guidelines and the Society's Privacy Policy.

(c) The Privacy Officer must receive the appropriate training, including training in the following:

i. the operations of the UBC Graduate Student Society,
ii. the requirements of the *BC Personal Information Protection Act*,
iii. the content of these Guidelines, the Society's Privacy Policy, the Society's Privacy Charts, and any other applicable documents,
iv. the terms of the GSS Access to Member Personal Information Memorandum of Understanding,
v. requesting a webinar training session from the BC Government, and obtaining certification in all of the following workshops
    1. Personal Information Protection Act (PIPA)
    2. Privacy Impact Assessments (PIAs), and
    3. Information Incidents, including Privacy Breaches
vi. completing the UBC Privacy & Information Security Fundamentals Training,
vii. reviewing the following, and any other applicable guidelines, issued by the Office of the BC Privacy Commissioner (OIPC BC),

1. A Guide to B.C.'s Personal Information Protection Act
2. Developing a Privacy Policy Under PIPA
3. Guide to the Personal Information Protection Act (BC Ministry of Citizens' Services)

viii. reviewing UBC's Encryption Guidelines,
ix. accessing legal counsel where necessary,
x. performing an annual Privacy Management Self-Assessment and other audits,
xi. conducing a Privacy Impact Assessment,
xii. responding to a privacy breach and privacy-related complaints per the protocol, and
xiii. training other employees on the Society's obligations under PIPA.

(d) The Privacy Officer must update all GSS privacy-related practices and documents annually where necessary, including this Guideline and the GSS Privacy Policy.

(e) The Privacy Officer may contact the OPIC BC for more information on their obligations under PIPA.

---

[1] See Centre for Humdata, "Introducing The Working Draft Of The OCHA Data Responsibility Guidelines" (2019), online: <centre.humdata.org/introducing-the-working-draft-of-the-ocha-data-responsibility-guidelines/>

[2] See University of British Columbia, Office of the Chief Information Officer, "Information Security Standard U1: Security Classification of UBC Electronic Information" (2021), online (pdf): <cio.ubc.ca/sites/cio.ubc.ca/files/documents/standards/Std%20U1%20Security%20Classification%20of%20UBC%20Electronic%20Information.pdf > ["Security Standard U1"]

[3] See Office of the Corporate Chief Information Officer, Enterprise Information Management, "Data and Information Security Classification Standard Guide" (2020), online (pdf): <imtpolicy.sp.alberta.ca/guidelines/pdf/Data-and-Information-Security-Classification-Guideline.pdf>

[4] See Office of the Information & Privacy Commissioner for British Columbia, *Green Planet Wholesale,* 2021 BCIPC 11, online: https://www.oipc.bc.ca/orders/3518

[5] See University of British Columbia, Office of the Chief Information Officer, "Information Security Standard U8: Destruction of UBC Electronic Information" (2021), online (pdf): <cio.ubc.ca/sites/cio.ubc.ca/files/documents/standards/Std%20U8%20Destruction%20of%20UBC%20Electronic%20Information.pdf>

[6] Office of the Information and Privacy Commissioner, "A Guide to B.C.'s Personal Information Protection Act for Businesses and Organizations Sources: OPC BC Guidelines" (2015), online (pdf): <www.oipc.bc.ca/guidance-documents/1438>; University of Toronto, *supra* note 11. (a–d); UBC Privacy Guidelines (e–f); UoT Guidelines (g)

[7] See Government of Alberta, Information Management and Technology, "Storing Data and Information", online (pdf): <imtpolicy.sp.alberta.ca/standards/pdf/Technical-Guide_Storing-Data-and-Information.pdf

[8] See Security Standard U1, *supra* note 2.

[9] See University of British Columbia, Office of the Chief Information Officer, "Information Security Standard U2: Passphrase and Password Protection" (2021), online (pdf): <cio.ubc.ca/sites/cio.ubc.ca/files/documents/standards/Std%20U2%20Passphrase%20and%20Password%20Protection.pdf>

[10] See Office of the University Counsel, "Privacy Fact Sheet: Privacy of Email Systems" (2015), online (pdf): < universitycounsel.ubc.ca/files/2015/05/Fact-Sheet-Privacy-of-Email-Systems.pdf>

[11] See University of Toronto, "Access and Privacy Practices: General and Administrative" (2011), online (pdf): <www.provost.utoronto.ca/wp-content/uploads/sites/155/2018/06/fippa.pdf>

[12] For more information on the privacy breach protocol for UBC-affiliated information, see University of British Columbia, Office of the Chief Information Officer, "UBC Incident Response Plan", online (pdf): <cio.ubc.ca/sites/cio.ubc.ca/files/documents/resources/UBC%20Incident%20Response%20Plan.pdf>

[13] For more information regarding an adequate complaints process, see BC Office of the Ombudsman, "Developing an Internal Complaint Mechanism" (2001), online (pdf): <bcombudsperson.ca/assets/media/Public-Report-No-40-Developing-an-Internal-Complaint-Mechanism.pdf>