Protection of Privacy Guideline

This guideline describes each of the seven privacy rules contained in the Freedom of Information and Protection of Privacy Act. It is intended to assist with interpreting and applying the Act during the course or executing the University’s business.

The seven rules are:

- collection
- accuracy
- correction
- use
- protection
- disclosure
- retention

Together, these rules form a Code of Fair Information Practices with which the University must comply.

1. Purpose for Which Personal Information may be Collected (Section 26)
2. How Personal Information is to be Collected (Section 27)
3. Accuracy of Personal Information (Section 28)
4. Correction of Personal Information (Section 29)
5. Protection of Personal Information (Section 30)
6. Retention of Personal Information (Section 31)
7. Use of Personal Information (Section 32)
8. Disclosure of Personal Information (Section 33)
9. Definition of Consistent Purposes (Section 34)

A. Collection, Accuracy, Protection and Retention of Personal Information

1. Purpose for Which Personal Information may be Collected (Section 26)

- Section 26 recognizes the University's legitimate need to collect personal information in order to carry out its mandate and to provide services, but restricts that collection to a defined set of circumstances.

- The circumstances are:
  - the collection of information is expressly authorized by or under an Act;
  - the information is collected for purposes of law enforcement; or
  - the information relates directly to and is necessary for the University's operating programs or activities.
• In the case of a University, the University Act only gives general authority for the University's educational program and we must then determine what exact elements of personal information we need to administer that program. The Act does not specify what elements can be collected.

• Under the powers conferred to the University President by the University Act, the University does collect, from time to time, law enforcement information in the form of investigations or proceedings that lead or could lead to a penalty or sanction being imposed.

• The University's operating program is any series of functions designed to carry out all or part of its mandate and an activity is an individual action designed to assist in carrying out an operating program.

• The University may do its own collection or may authorize an outside agent to carry out the collection on its behalf, either under contract or through an agreement or arrangement in writing with the other agency.

• Any written agreement or contract should stipulate that the protection, retention and disclosure of personal information will be governed by the Act.

• Unauthorized collection is when information is assembled or brought together and written down or recorded by any means (e.g. interview, questionnaire, survey, poll, audio tape, computer disk or tape, form, telephone call or letter) for purposes which are not allowed under section 26.

2. How Personal Information is to be Collected (Section 27)

• Section 27 promotes individuals' control over their personal information by requiring, with few exceptions, that personal information be collected directly from the person it is about unless another method of collection is authorized by the person.

• When collecting personal information about an individual from another source the authorization should be in writing; but, if it is given verbally the University should document the conversation and send a letter to the person concerned verifying the consent.

• When asking a person to give consent for indirect collection of personal information, s/he should be informed of:
  o the nature of the personal information to be collected;
  o the purpose of the indirect collection;
  o the reasons for making the collection indirectly; and
  o the consequences of refusing to authorize the indirect collection.

• The University may collect personal information indirectly only under the following conditions:
  o the information may be disclosed to the University under Sections 33 to 36 of the Act;
  o determining suitability for an honour or award, including an honourary degree, scholarship, prize or bursary;
  o collecting a debt or fine or making a payment; or
  o law enforcement.
• This section helps ensure that the University bases its decision about people on up-to-date, accurate and complete information.

• This section also allows the sharing of personal information within the University and in specific circumstances thereby reducing the response burden on individuals and allowing the University to make optimum use of personal information by eliminating costly duplicate collections wherever feasible.

• The Act imposes an obligation on the University to notify individuals of the purpose for which it is collecting the information, its legal authority for the collection and a contact person who can answer questions about the collection.

• Notice should be given at the beginning of a process either on the form used to collect the information or by giving the same notice to people at the beginning of an interview, mediation, conciliation, arbitration or inquiry process.

• The notification should be in writing wherever possible. If notification is done verbally, the University should follow up with a written notification to the person(s) concerned.

• The requirement to notify recognizes the individual's right to know and understand the purpose of the collection and how the information will be used. It also allows the person to make an informed decision as to whether or not to give the information in cases where a response is not mandatory.

• Where one person is asked for personal information about another person, the first person must also be informed of the purpose and authority for the collection of personal information about the second person.

3. **Accuracy of Personal Information (Section 28)**

• Section 28 requires that the University ensure that the personal information it collects and uses to make decisions about people is up-to-date, accurate and complete.

• This section recognizes that the University can have a profound effect on people's lives when it makes decisions about them using their personal information.

• This requirement applies only when the information is used to make a decision that will affect a person's life.

4. **Correction of Personal Information (Section 29)**

• Section 29 allows an individual to request that the University correct his/her personal information if there is an error or omission.
• If no correction is made the University must annotate the information with the correction that was requested.

• The University must notify any other person of the correction or annotation made who received the information during the past year.

• On receiving notice, the University must make the same correction or annotation.

5. Protection of Personal Information (Section 30)

• Section 30 requires the University to establish reasonable security measures for the personal information in its custody or control.

• Training and awareness about the Act's privacy rules, combined with appropriate physical and procedural security arrangements, help to ensure that personal information is not released, used, handled or destroyed in unauthorized ways.

• Employees, contractors and others who are authorized to handle personal information must not only be aware of the need to provide appropriate protection of the personal information they use, they must actually comply with the security standards.

• After training, compliance with security standards is monitored to ensure that physical and procedural security precautions are established and remain at appropriate levels.

• Reasonable security arrangements means taking measures that are appropriate to the sensitivity and volume of the information and the medium in which it is stored, transmitted, handled or transferred.

• Examples of physical security measures include:
  o locked doors and filing equipment;
  o electronic access control device;
  o location of FAX machine in a secure area;
  o positioning of computer terminals so that screens cannot be seen by passers-by;
  o receptionist supervision;
  o after hours security patrol checks;
  o anonymous labeling on file drawers, boxes and other storage containers;
  o open filing equipment or mail boxes kept behind a counter or other physical barrier to the public;
  o secure transportation or transmission.

• Examples of procedural security measures include:
  o computer access codes;
  o controlled distribution of keys, combinations or codes;
  o segregation of confidential information;
  o a clean desk policy;
  o file check-out procedures;
- designation of personnel with authorized access or level of access;
- phoning to confirm receipt of a FAX message containing sensitive information;
- security provisions in service contracts to destroy records.

- Appropriate safeguards are implemented over time and within available resources, following an assessment of the types and level of sensitivity of personal information.

- Unauthorized access is when University employees or members of the public have access to personal information where they do not need to see or handle it in the course of their employment or other duties.

6. **Retention of Personal Information (Section 31)**

- Information used to make a decision that directly affects an individual must be retained for at least one year after use.

- This ensures that people have adequate time to exercise their right to request access, know the uses and disclosures that were made of their personal information, verify that decisions about them were not based on wrong or out-of-date information and allows them to request the correction of any mistakes or missing information.

- The University makes a decision about a person when it uses personal information that has an effect on the person concerned; for example, deciding a student's eligibility for admission; determining a person's qualification for a job; evaluating someone's job performance for tenure, promotion or renewal; assessing a student's request for accommodation services, deciding an applicant's eligibility for financial assistance; etc.

- The University can keep personal information longer than one year, depending on its operational needs.

- Personal information should not be retained for an indefinite time period because this increases the potential that out-of-date and incomplete information would be available for use and it increases the opportunities for unauthorized access or disclosure.

- Personal information can be stored in a location other than the office that received it (i.e. the University Records Centre or a shared server).

- It is not necessary to retain personal information that has been used solely for research or statistical purposes where no decision will be made about the respondents. For example, a survey gathers personal information to study trends or gather opinions and is then rendered anonymous when rolled up into an aggregate form; therefore, the original survey instruments may be destroyed as soon as the desired information has been extracted.

- Retaining personal information means not disposing of it by destroying or transferring it.
• Authorized disposal may be either transfer of the record to the legal custody and control of the University Archives or physical destruction of the record containing personal information in such a way that it cannot be retrieved or reconstructed.

• A record should be kept of the information destroyed or transferred to the Archives.

• Unauthorized disposal of personal information means disposing of records containing personal information, either without the approval of the designated authority or in ways which do not adhere to approved methods and standards.

B. Use and Disclosure of Personal Information

1. Use of Personal Information (Section 32)

• This section governs the access and use of personal information within the University for a specific program function.

• Section 32 restricts uses of personal information to:
  o that for which the information was collected;
  o a consistent use (one which is related directly to the original use);
  o one to which the person concerned has consented; or
  o purposes for which the information may be disclosed under sections 33 to 36.

• This section balances the person's right to control the uses to which the University puts her or his information against the need of the University to make optimum use of the personal information in its custody or control by:
  o eliminating duplicate collection for new uses;
  o reducing the person(s) response burden and the financial costs of repeated collections for new uses; and
  o promoting the efficiency of the University.

• An essential element in this increased control is the requirement that the University obtain the consent of the person concerned for any new use which was not specifically authorized by the original purpose, a consistent purpose or section 33 to 36.

• The person must consent to the new use in accordance with the requirements set out by Regulation, that is, in writing and specifying to whom the personal information may be disclosed and how it may be used.

• Use of personal information means employing it to accomplish the University's objectives, for example, to administer a program or activity, to provide a service or to determine someone's eligibility for a benefit or suitability for a job.

• The purpose of the collection is the reason for which the information is needed and the use(s) that a public body will make of the personal information.
• The purpose for which information is collected is the object to be attained by the collection of the information or the thing intended to be done, that is, the administration of programs, provision of services and other activities described as uses.

• The purpose must conform with the authority to collect the information, that is, expressly authorized by legislation or where it is needed to administer a specific program or activity.

• Consistent use means directly related to the original use and that is necessary to perform the statutory duties or operating a legally authorized program of the University.

• A record must be kept of any inconsistent use of personal information.

• Unauthorized use is using the information to serve a purpose which is not permitted under section 32.

2. Disclosure of Personal Information (Section 33)

• This section governs the disclosure of personal information to any person or body outside the program which collected the information.

• This section acknowledges that the University is sometimes required to disclose personal information to third parties in order to administer its programs, but restricts the disclosure to the situations permitted in sections 33 to 36.

• Section 33 requires the consent of the person concerned for disclosure of his/her personal information in circumstances other than those permitted under sections 33 to 36. In doing so, it safeguards against the disclosure of personal information for uses which were never intended by the people concerned, of which they may not have been aware and which they would not permit if they were aware.

• Wherever possible, the University should obtain consent for all anticipated disclosures at the time that it collects the information.

• The absence of consent is interpreted as the absence of authorization. Where the person has not consented to a disclosure of personal information, the University cannot assume consent to the new disclosure.

• Disclosure is permitted if the person is aware of the specific information to be disclosed and has been informed of the new use to which the information will be put and of the consequences of agreeing or refusing to the disclosure. By giving consent, the person acknowledges s/he knows and understands the consequences of the disclosure and has made an informed decision about whether or not to agree to it.

• The University may disclose personal information if it is necessary to do so in order to accomplish the purpose for which the personal information was originally collected.
• Disclosure for consistent use is permissible if it is directly connected to the original use or is a logical extension of the original use.

• The University may disclose personal information to an officer or employee within the University who must need to see it in order to do their jobs. An employee is a person employed by the University and includes a person retained under contract to perform services for the University.

• Personal information must not be disclosed to be used for mailing lists, solicitations by telephone or other means. This is defined as sending similar information, making requests or petitions in a systematic manner by mail, telephone, door-to-door or facsimile transmission.

• A record must be kept of any inconsistent disclosure of personal information.

• Unauthorized disclosure is revealing, exposing, showing, providing copies of, selling, giving or telling personal information in ways that section 33 does not permit.

3. Definition of Consistent Purposes (Section 34)

• Consistent use means that the new use or disclosure must be directly connected to the original purpose and essential to the execution of the University's mandate.

• Consistent use must have a logical and plausible link to the original purpose. It must flow or be derived directly from the original use or be a logical outgrowth of the original use.

• There is no strict rule on what constitutes a consistent use. One guideline to consider is whether the person concerned would expect the personal information to be used in the proposed way, even if that use has not been spelled out.

For further explanation or clarification on the application of the Freedom of Information and privacy Act, contact the SFU Privacy Officer

sfu.ca/archives