University of Victoria

Protection of Privacy Policy

University Policy No: GV0235
Classification: Governance
Approving Authority: Board of Governors
Effective Date: July 2018
Supersedes: June 2017
Last Editorial Change:
Mandated Review: June 2020

Associated Procedures:
Procedures for Responding to a Privacy Incident or Privacy Breach
Procedures for the Management of University Surveillance Systems
Procedures for the Disclosure of Student Personal Information in Emergency or Compelling Circumstances
Procedures for the Management of Personal Information
University Information Security Classification Procedures
Procedures for Responding to the Loss or Theft of a Mobile Computing Device

---

PURPOSE

1.00 This policy articulates how the university complies with the privacy components of the *Freedom of Information and Protection of Privacy Act* (FIPPA).

DEFINITIONS

2.00 **Administrative Authority** means individuals with administrative responsibility for Units including but not limited to: Vice-Presidents, Associate Vice-Presidents, Deans, Chairs, Directors, Executive Directors, the Chief Information Officer, and other Unit Heads.

3.00 **Consistent Purpose** means a use or disclosure of Personal Information which is consistent with the purposes for which the information was obtained or compiled if the use or disclosure:
(a) has a reasonable and direct connection to that purpose, and
(b) is necessary for performing the statutory duties of, or for operating a legally authorized program of, the Unit that uses or discloses the information or causes the information to be used or disclosed.

4.00 **Contact Information** means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual.

5.00 **Disclose** means to transmit or provide, intentionally or unintentionally, Personal Information by any means to someone other than an Employee.

6.00 **Employee** in relation to the university, includes a volunteer and a service provider.

7.00 **Monitor/Monitored** (*verb*) means a Surveillance System is used to view live footage of an area without creating a record of that observation.

8.00 **Personal Information** means recorded information about an identifiable individual other than Contact Information.

9.00 **Privacy Impact Assessment** means an assessment that the university conducts to determine if a current or proposed system, project, program or activity meets or will meet FIPPA's privacy protection requirements.

10.00 **Record** (*noun*) includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records.

11.00 **Record/Recorded** (*verb*) means a Surveillance System is used to convert images and/or sound into a record that can be reproduced.

12.00 **Surveillance System** means an analog or digital video recording system (with or without audio) authorized and used by the university intended to monitor or record the activities of people or monitor or record an area that is accessible to the university community or public. For the purposes of this policy and its associated procedures, surveillance does not include the use of personal video equipment or the recording or broadcasting of public events, educational activities, or recordings done through UVic Audiovisual and Multimedia Services.

13.00 **Unit** means academic or administrative areas at the university, including but not limited to: faculties, departments, divisions, offices, schools and centres.

14.00 **Use of Personal Information** means employing or handling Personal Information by Employees to accomplish the university's objectives; for example, to:

- administer a program or activity;
- provide a service; or
- determine someone's eligibility for a benefit or suitability for a job.

JURISDICTION/SCOPE

15.00 This policy applies to all Employees (including faculty), students and Units. It applies to all Personal Information in the custody or under the control of the university.

POLICY

16.00 The university will manage all Personal Information in accordance with the FIPPA, the *University Act*, collective agreements, contracts, and this and other applicable university policies and associated procedures.

Accountability for Personal Information

17.00 The President will designate a senior administrator to act as head under the FIPPA who will be responsible for the administration of the FIPPA and this policy.

17.01 The General Counsel has been designated by the President as the head.

General Counsel

18.00 As the head, the General Counsel is responsible for the overall co-ordination of privacy and access functions.

18.01 The General Counsel will carry out their duties in collaboration with the University Secretary and the University Archivist, who are responsible for the maintenance of the university's Records management program.

Chief Privacy Officer

19.00 In collaboration with the University Secretary, the University Archivist, and the Chief Information Officer, the Chief Privacy Officer is responsible for promoting, monitoring, and reporting on compliance with the FIPPA and with university privacy, records management, and information security policies. The Chief Privacy Officer's responsibilities include:

- Providing privacy advice and training;
- Providing ongoing assessment of privacy risks; and
- Responding to privacy complaints and investigating concerns about privacy issues.

19.01 Where the Chief Privacy Officer establishes that there is a significant privacy risk, the Chief Privacy Officer may investigate and/or recommend to the appropriate Administrative Authority corrective action, suspension, or termination of a project or activity.

Administrators

20.00 Administrative Authorities and managers are responsible for:

- making reasonable efforts to familiarize themselves with the requirements in the FIPPA, this policy and its associated procedures, and for making reasonable efforts to communicate these requirements to the Employees in their Units;
- making reasonable efforts to ensure that the management of Personal Information in the custody or under the control of their units meets the requirements of the FIPPA, this policy and its associated procedures;
- reporting any privacy incidents or breaches of the FIPPA, this policy or its associated procedures in accordance with the university's Procedures for Responding to a Privacy Incident or Breach; and
- Conducting risk-based privacy impact assessments under s. 42.00.

Employees

21.00 All Employees who collect, access, use, disclose, maintain and dispose of Personal Information are in a position of trust.

21.01 Employees are responsible for:

- treating all Personal Information to which they receive access in accordance with the FIPPA and this policy;
- making reasonable efforts to familiarize themselves and to comply with the requirements in the FIPPA, this policy, and its associated procedures;
- consulting as necessary with the appropriate authority regarding the requirements in the FIPPA, this policy, and its associated procedures; and
- reporting any privacy incidents or breaches of the FIPPA, this policy, or its associated procedures in accordance with the university's Procedures for Responding to a Privacy Incident or Breach.

Third Parties

22.00 The university will require a third party service provider whose work on behalf of the university involves the collection, use or Disclosure of Personal Information to abide by this policy, the Privacy Protection Schedule, and FIPPA in its handling of personal information on behalf of the university, and may require the service provider to sign a confidentiality agreement.

Openness about Personal Information Policies and Practices – Collection Notice

23.00 The university will make the following information available to an individual from whom Personal Information is being collected:

(a) the purpose for which the Personal Information is being collected;
(b) the legal authority to collect the Personal Information; and
(c) the Contact Information of someone who can provide details about the collection.

24.00 This policy will be made available on the university website.

Identifying Purposes for Personal Information

25.00 The university collects Personal Information from students, Employees and others in order to fulfill its mandate under the *University Act*.

25.01 The university collects Personal Information as authorized by the FIPPA and the *University Act*, including collecting Personal Information that relates directly to and is necessary for an operating program or activity of the university.

Consent for Collection of Personal Information

26.00 The university will normally obtain either express or implied consent from an individual before collecting Personal Information, but may collect, use or disclose Personal Information without consent in limited circumstances where the FIPPA authorizes such activity.

Limiting Collection of Personal Information

27.00 The university will normally collect Personal Information directly from the individual whom the Personal Information is about, but may collect Personal Information indirectly in limited situations where such collection is authorized by the FIPPA, another enactment, or the individual.

27.01 The university may also collect Personal Information indirectly for purposes of:

(a) determining suitability for an honour or award, including an honorary degree, scholarship, prize or bursary;
(b) a proceeding before a court or a judicial or quasi-judicial tribunal;
(c) collecting a debt or fine or making a payment;
(d) law enforcement; or
(e) any other purposes permitted by law.

Use, Disclosure, and Retention of Personal Information

28.00 The university uses and discloses the Personal Information in its custody or under its control:

(a) for the purpose for which that information was obtained or compiled or for a Consistent Purpose;
(b) in a manner to which an individual has consented;
(c) as permitted or required by the FIPPA or as authorized or required by other law;
(d) for research and statistical purposes; or
(e) for archival or historical purposes.

29.00 Employees must only seek to access and use Personal Information necessary for the performance of their duties.

30.00 Employees may allow other Employees to use Personal Information needed for the performance of their duties. Employees may also allow other Employees to use Personal Information if the FIPPA authorizes the use of that Personal Information.

30.01 If an Employee is in doubt whether to allow another Employee to use Personal Information, the Employee will consult with their Administrative Authority or manager as necessary.

31.00 The university will disclose Personal Information to students and individuals or organizations outside the university as permitted by the FIPPA, as authorized or required by an enactment, as permitted by this policy and its associated procedures.

31.01 Personal Information shall only be disclosed in compliance with the Procedures for the Management of Personal Information.

31.02 If an Employee is in doubt whether to disclose Personal Information, the Employee will consult with their Administrative Authority as necessary.

32.00 Disclosure of the following information without consent is permitted:

(a) an Employee's Contact Information;
(b) information about an individual's position, functions, or remuneration as an officer, Employee, or member of the university;
(c) names of individuals who have received degrees, the names of degrees those individuals received and the years in which the degrees were awarded; and

(d) Personal Information about an individual in an emergency situation or where the General Counsel (or designate) determines that compelling circumstances exist that affect anyone's health or safety, or as permitted by the Procedures for Disclosure of Student Information in Emergency or Compelling Circumstances.

33.00 Disclosing Personal Information outside Canada must be done in compliance with FIPPA and the Procedures for the Management of Personal Information.

34.00 The university will retain Personal Information collected from individuals in accordance with the FIPPA and the university-wide records classification, retention and disposition plan.

34.01 The university will retain Personal Information used to make a decision about an individual for a minimum of one year.

35.00 The university may use Surveillance Systems to:

(a) improve personal safety on university property by acting as a deterrent or increasing the likelihood of identifying individuals who may commit criminal activity;
(b) assist law enforcement agencies with the investigation of any suspected criminal activity;
(c) assist with the protection of university assets and infrastructure; or
(d) assist with the application of university policies.

35.01 Surveillance Systems shall not be used to monitor or record areas where the university community or public have a reasonable expectation of privacy.

35.02 The university will deploy Surveillance Systems only as an exceptional step to address real, pressing and substantial problems or risks and only where a less privacy-invasive alternative is not available. Surveillance Systems will be designed to minimize the impact on privacy. The privacy impact of the proposed Surveillance System will be assessed and documented in the Privacy Review Form.

35.03 Approval is required prior to installation of a Surveillance System. The General Counsel is responsible for approval of the installation, following input from the Vice-President Finance and Operations and confirmation that the installation is necessary to address real, pressing and substantial problems or risks and that a less privacy-invasive alternative is not available.

35.04 The requisite Vice-President may delegate the day-to-day operations and administration of the Surveillance System in accordance with the Procedures for the Management of University Surveillance Systems.

36.00 In accordance with the Procedures for the Management of University Surveillance Systems, the university will provide notice of the use of Surveillance Systems by prominently displaying signage at the perimeter or entrance to the area being monitored

or recorded to alert individuals that such systems are or may be in use before they enter any area under surveillance.

37.00 Sections 35.00 and 36.00 apply only to Surveillance Systems installed with notice, i.e., overt surveillance.

Ensuring Accuracy of Personal Information

38.00 The university will make every reasonable effort to ensure that the Personal Information in its custody or under its control is accurate and complete and will allow Employees and students to confirm the accuracy of this information.

38.01 Procedures for the correction of Personal Information are contained within the university's Procedures for the Access to and Correction of Information.

Safeguards for Personal Information

39.00 The university will protect Personal Information in its custody or control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposition.

Individual Access to Personal Information

40.00 Individuals have a right to access Personal Information about themselves, subject to exceptions under the FIPPA. Access to Personal Information is provided in accordance with the university's Access to and Correction of Information procedure.

41.00 Individuals have a right to request corrections to Personal Information about themselves, subject to exceptions under the FIPPA. Corrections to Personal Information are provided in accordance with the university's Access to and Correction of Information procedure.

Privacy Impact Assessments

42.00 The Administrative Authority must conduct a risk-based Privacy Impact Assessment for all new systems, projects, programs or activities and substantially modified systems or activities. The nature and extent of the assessment will be based upon the risk.

42.01 Before committing the university to a project or initiative or before procurement that may entail privacy risks, the Administrative Authority will assess the project or initiative for potential privacy risks.

42.02 Upon completion of the PIA, an appropriate Administrative Authority, which may be the same Administrative Authority that completed the PIA, will determine whether the project's risk after mitigation shall be accepted, or whether the project should not proceed.

42.03 In 42.02 the appropriate Administrative Authority will be determined under the Procedures for the Management of Personal Information. This determination will be based on the magnitude of the risk which is determined by impact and likelihood of the risk.

Challenging Compliance with the Privacy Policy

43.00 Individuals are entitled to challenge the university's compliance with this policy.

43.01 Employees who receive a complaint or inquiry about compliance with the policy should attempt to resolve the issue with the assistance of a supervisor.

43.02 Individuals may make a formal complaint or inquiry about compliance with this policy by contacting the Privacy and Access Office.

General

44.00 The General Counsel may waive the requirements in sections 22.00 and 42.00 in exceptional circumstances.

AUTHORITIES AND OFFICERS

I. Approving Authority: Board of Governors
II. Designated Executive Officer: President
III. Procedural Authority: President
IV. Procedural Officer: General Counsel

RELEVANT LEGISLATION

University Act
Freedom of Information and Protection of Privacy Act

RELATED POLICIES AND DOCUMENTS

Associated Procedures

- Procedures for Responding to a Privacy Incident or Privacy Breach
- Procedures for the Management of University Surveillance Systems
- Procedures for the Disclosure of Student Personal Information in Emergency or Compelling Circumstances
- Procedures for the Management of Personal Information
- University Information Security Classification Procedures
- Procedures for Responding to the Loss or Theft of a Mobile Computing Device

Records Management Policy (IM7700)

- Procedures for the Access to and Correction of Information
- Procedures for the Management of University Records
- Guidelines for the Secure Destruction and Deletion of University Records and Information

Information Security Policy (IM7800)

- Procedures for Responding to an Information Security Incident

Directory of Records

EXTERNAL RESOURCES

Canadian Standards Association Privacy Code

University of Victoria

PROCEDURES FOR RESPONDING TO A PRIVACY INCIDENT OR PRIVACY BREACH

Procedural Authority: President
Procedural Officer: General Counsel
Parent Policy: Protection of Privacy Policy (GV0235)

Effective Date: June, 2017
Supersedes: January, 2010
Last Editorial Change: July 2018

PURPOSE

1.00 The purpose of this document is to set out response procedures to be followed when a Privacy Incident or Privacy Breach occurs at the university.

DEFINITIONS

2.00 The definitions contained within the university's Protection of Privacy policy (GV0235) apply to these procedures.

3.00 **Privacy Breach** refers to a confirmed case of unauthorized access to or collection, use, disclosure or disposition of Personal Information. Such activity is considered to be 'unauthorized' if it occurs in contravention of the *Freedom of Information and Protection of Privacy Act,* or the University's Protection of Privacy Policy (GV0235).

4.00 **Privacy Incident** means an unconfirmed but potential Privacy Breach.

5.00 **Unauthorized Disclosure** means the disclosure of, production of or the provision of access to Personal Information to which the *Freedom of Information and Protection of Privacy Act* applies, if that disclosure, production or access is not authorized under the *Freedom of Information and Protection of Privacy Act*.

SCOPE

6.00 These procedures apply to Employees of the university (including faculty).

Statutory and Policy Authority

7.00 In accordance with the *Freedom of Information and Protection of Privacy Act* (FIPPA); an Employee or service provider who is aware of an unauthorized disclosure of Personal Information must immediately notify the General Counsel, delegated head of the public body.

7.01 In accordance with the university's Protection of Privacy policy (GV0235), employees are responsible for reporting any breaches of FIPPA or the policy to the appropriate Administrative Authority or manager or the General Counsel. Administrative Authorities or managers are responsible for reporting any breaches of FIPPA or the policy to the General Counsel.

PROCEDURES

There are several stages when responding to a report of Privacy Incident or Privacy Breach. While the stages are listed sequentially, activities from various stages may overlap depending upon the nature of the Privacy Incident or Privacy Breach.

Identification and Reporting

8.00 Privacy Incidents may be identified at any level of the university through:

- responding to Personal Information complaints;
- monitoring the use of systems;
- reporting of security incidents under the procedures for Responding to an Information Security Incident (Under Development); or
- reporting from external sources.

9.00 Individuals who are aware of a Privacy Incident or Privacy Breach shall immediately report the Privacy Incident or Privacy Breach to the Privacy and Access Office by calling (250) 472-4914or e-mailing foipp@uvic.ca using the subject line – "Privacy Incident".

Initial Assessment and Internal Reporting

10.00 The Privacy and Access Office will initially assess the cause, severity and risk of the Privacy Incident or Privacy Breach. Such assessment will determine future actions including whether to assemble a response team.

11.00 Where it appears to the General Counsel that there may be or has been a substantial Privacy Incident or Privacy Breach, or the Incident or Breach may or does involve highly-sensitive Personal Information, the General Counsel (or designate) will inform the requisite Vice-President (or designate) and may notify the President as appropriate.

12.00 Where there has been a report to the Privacy and Access Office of an unauthorized disclosure of information involving university systems but not involving Personal Information, the General Counsel will inform the Chief Information Officer (or designate).

Containment

13.00 The requisite Unit(s) is responsible to make reasonable efforts to immediately contain the Privacy Incident or Privacy Breach by, for example:

- stopping the unauthorized practice;
- recovering the Record(s) or information that was improperly collected, used, disclosed, or disposed of;
- shutting down affected systems;
- revoking access;
- changing computer access codes;
- blocking network access; or
- correcting weaknesses in physical security.

Risk Assessment

14.00 The General Counsel on receipt of a report of a Privacy Incident or Privacy Breach, if warranted, will immediately assemble a response team that may include, but is not limited to the following individuals (or their designates):

- the General Counsel;
- the Vice-President Finance and Operations;
- the University Chief Privacy Officer;
- the University Secretary;
- the Executive Director of University Communications + Marketing;
- the Chief Information Officer (if the Privacy Incident or Privacy Breach involves information systems); and
- the head of the Unit responsible for the Personal Information involved:
    - for employee information either the Executive Director, Financial Services or Associate Vice-President Human Resources;
    - for student information the Registrar; or
    - for Faculty information, the Dean of the Faculty.

14.01 In certain cases involving stolen property or other unlawful activity, Campus Security may also be added to the response team.

15.00 Where formed, the response team will review the report and assess the risk posed by the Privacy Incident or Privacy Breach by:

- Confirming the Personal Information involved;
- Determining whether the incident is a Privacy Breach;
- Determining the cause and extent of the Privacy Incident or Privacy Breach;
- Confirming the individuals potentially affected by the Privacy Incident or Privacy Breach;
- Assessing the potential harm from the Privacy Incident or Privacy Breach.

Notification

16.00 The response team will recommend to the General Counsel the scope and nature of the notification and will examine:

- the need to notify the affected individual(s);
- the method and timing of notification;
- the need to notify other external parties (such as the Office of the Information and Privacy Commissioner or the police).

17.00 The General Counsel will determine the necessary notification and issue the notification based on the response team's recommendation. Where time permits, the General Counsel will inform the Administrative Authority responsible for the Unit in advance of the notification.

Follow-up and Prevention

18.00 Once the steps are taken to mitigate the risks associated with the Privacy Breach, upon the recommendation of the response team, the General Counsel will determine whether further investigation of the cause of the Privacy Breach is necessary.

19.00 The response team will conduct any further investigation, which may require a security audit of physical and technical security. As a result of this evaluation, the response team may recommend necessary safeguards against further Privacy Incidents or Privacy Breaches. Existing policies, procedures and practices may be reviewed and updated to reflect the lessons learned from the investigation.

20.00 The Administrative Authority of the affected Unit is responsible for reporting to the General Counsel its response to and implementation of the response team's recommendations. The General Counsel may also recommend follow-up actions to the President or the requisite Vice-president.

RELEVANT LEGISLATION

Freedom of Information and Protection of Privacy Act

RELATED POLICIES AND DOCUMENTS

Protection of Privacy Policy (GV0235)

- Procedures for the Disclosure of Personal Information in Emergencies and Compelling Circumstances
- Procedures for the Management of University Surveillance Systems
- Procedures for the Management of Personal Information
- Procedures for Responding to the Loss of Theft of a Mobile Computing Device
- University Information Security Classification Procedures
- Privacy Protection Schedule

Records Management Policy (IM7700)

- Procedures for Access to and Correction of Information
- Procedures for the Management of University Records
- Guidelines for the Secure Destruction and Deletion of University Records and Information

Information Security Policy (IM7800)

- Procedures for Responding to an Information Security Incident

University of Victoria

PROCEDURES FOR THE MANAGEMENT OF UNIVERSITY SURVEILLANCE SYSTEMS

Procedural Authority: President
Procedural Officer: General Counsel
Parent Policy: Protection of Privacy Policy (GV0235)

Effective Date: July 2018
Supersedes: June, 2017
Last Editorial Change:

PURPOSE

1.00 The purpose of these procedures is to set out how the university manages the Personal Information collected as a result of the installation and use of Surveillance Systems.

DEFINITIONS

2.00 The definitions contained within the university's Protection of Privacy (GV0235) policy apply to these procedures.

PROCEDURES

3.00 The university installs and uses Surveillance Systems in accordance with the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the university's Protection of Privacy policy (GV0235).

4.00 A Privacy Review Form must be submitted to the Vice-President Finance and Operations for review and input prior to the approval of the installation of a Surveillance System. The completed form and Vice-President Finance and Operations' input will be forwarded to the General Counsel for consideration.

5.00 If installation is approved by the General Counsel, the responsible vice-president may delegate the management of a Surveillance System to an appropriate Administrative Authority. The Administrative Authority may assign to an appropriate individual the supervision of the daily operations and the administration of the operations of the Surveillance System.

Set-up of Surveillance Systems

6.00 Surveillance System equipment must only be purchased from and installed by suppliers approved by the university.

6.01 Purchasing and installation of Surveillance Systems are subject to the university purchasing policies and procedures.

7.00 Areas chosen for surveillance and the location of the Surveillance System must be necessary to meet the purposes approved by the General Counsel at the time of the application for installation. The Surveillance System must be installed in such a way (e.g., angle, breadth and depth of field) so as to achieve the minimal collection of Personal Information, while meeting the approved purposes for the installation.

7.01 Individuals have a reasonable expectation of privacy in areas such as washrooms, change rooms, offices, and university residences.

7.02 Surveillance Systems shall not be directed to look through the windows of adjacent buildings.

8.00 Surveillance systems must follow standards established by Campus Security and University Systems.

9.00 Only authorized individuals shall have access to use the Surveillance System's controls and reception equipment for monitoring. Only the Director of Campus Security (or designate) shall review Surveillance System recordings, have physical access to recording equipment, approve who is permitted to use Surveillance Systems for monitoring, and approve access to recordings under section 22.00.

10.00 Reception equipment (such as video monitors or audio playback speakers) will be in a controlled access area.

11.00 Video monitors must not be located in a position that enables public viewing.

12.00 Information recorded by a Surveillance System may only be used for the purposes outlined in section 35.00 of the Protection of Privacy policy (GV0235).

Signage

13.00 If the Surveillance System will be used to monitor an area, the following sign will be displayed:

This area is being MONITORED by a Surveillance System.

14.00 If the Surveillance System will be used to record an area, the following sign will be displayed:

This area is being RECORDED by a Surveillance System.

15.00 If the Surveillance System is recording and being monitored, the following sign will be displayed:

This area is being RECORDED and may be MONITORED by a Surveillance System.

16.00 In addition to the above signage statements, each sign will also include a contact for inquires about the Surveillance. The following wording must appear on the bottom of the sign:

> *The university collects personal information through its Surveillance System, authorized and installed under the Protection of Privacy Policy. Further information may be obtained from the Privacy and Access Office at (250) 472-4914.*

Management of Surveillance Recordings and Media

17.00 Surveillance recordings will be kept for a maximum of thirty (30) days unless required for the purposes outlined in section 35.00 of the Protection of Privacy (GV0235) policy.

17.01 If a recording has been used to make a decision about an individual, that recording will be retained for one year after the decision in accordance with FIPPA and the Protection of Privacy policy (GV0235).

17.02 If a recording is needed for an investigation or legal proceeding, it may be retained for as long as required for that purpose.

18.00 All storage media containing Surveillance System recordings shall be stored securely in a controlled access area.

19.00 If Surveillance System recordings are kept on removable storage media, such as tapes, CDs, DVDs, or USB sticks, then the media must be labeled numerically. They must also be labelled with the dates, times, and locations that the recordings have captured. Back-ups will be kept in the event that a recording has to be removed for examination or evidentiary purposes. Back-ups shall have the same labelling and the same access restrictions as original recordings.

20.00 If Surveillance System recordings are kept on computer storage media, the recordings must be created as separate files, at least one file per day, and must be overwritten or otherwise made permanently unreadable on or before the maximum retention period stated in sections 17.00 to 17.02. Any back-up of such files shall be in a secure manner.

21.00 Recording media used for Surveillance Systems that is no longer required shall be destroyed in accordance with the University's Guidelines for the Secure Destruction and Deletion of University Records and Information .

Access to Surveillance Recordings

22.00 Access to Surveillance System recordings requires an incident number from Campus Security. The Director of Campus Security (or designate) will determine the degree of access and any use or disclosure that is permitted. This use or disclosure shall be on a "need to know" basis as determined by the Director of Campus Security (or designate).

23.00 Access to and use of Surveillance System recordings shall be logged in accordance with Campus Security procedures.

24.00 All disclosures of Surveillance System recordings shall comply with the Procedures for the Management of Personal Information.

Incident Response

25.00 When an area under surveillance is being monitored or recorded by an authorized individual, and this individual has reason to believe that an incident is occurring or has occurred that threatens safety or property, or is criminal in nature, or is a serious violation of university policy, the authorized individual will immediately contact Campus

Security. Only Campus Security may review surveillance recordings. If Campus Security has reason to believe that such an incident has occurred, Campus Security may notify the following as required:

- in circumstances involving a student – the Associate Vice-President Student Affairs;
- in circumstances involving a faculty member – the Associate Vice-President Faculty Relations and Academic Administration;
- in circumstances involving a staff member – the Associate Vice-President Human Resources;
- in circumstances involving a visitor – Vice-President External Relations.

In cases of suspected criminal activity, Campus Security will contact the police as required.

26.00 Surveillance recordings will only be removed or copied when an incident has been identified. In such a case, Campus Security will secure and take control of the recording in question. No other copies of such recordings will be made other than for back-up or evidentiary purposes.

27.00 When an incident occurs, Campus Security will provide an incident report to the authorized individual. The authorized individual shall inform the requisite Administrative Authority that Campus Security has secured and taken control of the recording.

Individual Access to Recordings

28.00 Where an individual has been recorded by a Surveillance System, the individual, after identifying the time and location of the recording, has the right to request access to their recorded Personal Information. Such access in full or part may be refused on one of the grounds set out in FIPPA. However, if the information can reasonably be severed from a record, the individual has the right of access to the remainder of the record.

Audits

29.00 The university may ensure that periodic audits are conducted to ensure compliance with this procedure and related aspects of the Protection of Privacy policy (GV0235). The results of each audit will be documented.

30.00 The Office of the Information and Privacy Commissioner may conduct audits of the university's Surveillance Systems.

RELEVANT LEGISLATION

University Act
Freedom of Information and Protection of Privacy Act

RELATED POLICIES AND DOCUMENTS

Protection of Privacy Policy (GV0235)

- Procedures for the Management of Personal Information
- Procedures for Responding to a Privacy Incident or Privacy Breach

Records Management Policy (IM7700)

- Guidelines for the Secure Destruction and Deletion of University Records and Information

University of Victoria

PROCEDURES FOR THE DISCLOSURE OF STUDENT PERSONAL INFORMATION IN EMERGENCY OR COMPELLING CIRCUMSTANCES

Procedural Authority: President
Procedural Officer: General Counsel
Parent Policy: Protection of Privacy Policy (GV0235)

Effective Date: June, 2017
Supersedes: January, 2010
Last Editorial Change: July 2018

PURPOSE

1.00 The purpose of this document is to set out procedures for circumstances where there is concern for the health or safety of a student or others at the university and it is not possible to obtain the student's consent to use or disclose their Personal Information.

Note: For further guidance on the management of urgent or emergency circumstances, see the university's Environmental Health and Safety policy (SS9200) and the Critical Incident Response Procedures (SS9115).

DEFINITIONS

2.00 The definitions contained within the university's Protection of Privacy policy (GV0235) apply to these procedures.

3.00 Compelling Circumstances exist where one is compelled to act to protect an individual whose health or safety is in imminent danger.

4.00 Emergency means a present or imminent event of a short duration that affects or threatens: the health, safety or welfare of people, property and infrastructure, and or the purposes of the university.

5.00 Threatening Behaviour means any statement or conduct which may cause a reasonable person to believe that:
(a) the personal safety of any person is endangered; or
(b) property is at risk of damage, destruction or loss other than the authorized use or destruction of university property; or
(c) a person has acted in a manner or is engaged in a course of conduct reasonably likely to result in risk to property or danger to anyone's personal safety as in paragraphs (a) or (b) above.

6.00 Urgent incidents are those which may include incidents:
(a) of persons in extreme emotional distress;
(b) involving sudden trauma or death;
(c) of inter-personal conflict; and
(d) of other matters similar in nature.

PROCEDURES

7.00 The university is committed to maintaining an environment where all members of the university community and the public may participate safely in the university's activities. The paramount principle, preservation of life trumps privacy will be considered as a starting point in protecting health and safety as effectively as possible when making difficult judgment decisions.

8.00 In accordance with the university's Protection of Privacy Policy (GV0235), Personal Information may be used or disclosed as permitted or required by the *Freedom of Information and Protection of Privacy Act* (FIPPA) or other law, and in Emergency situations.

9.00 Under normal circumstances, disclosure of Personal Information is handled through consent (either expressed or implied) and, within the university; its use is limited to those who need to know the information in order to discharge their university duties.

Disclosure of Personal Information in Emergencies

10.00 When a university faculty or staff member is faced with circumstances where the normal consent and other routes authorized by statute for disclosure are not available and where there is an Emergency, the staff member shall disclose Personal Information as relevant and necessary to campus security.

11.00 When a university faculty or staff member is faced with circumstances where the normal consent and other routes authorized by statute for disclosure are not available and where there is an Urgent need to contact the emergency contact person or the next-of-kin of an ill, injured or deceased student, contact may be initiated by the staff or faculty member.

In the case of a deceased student, refer to the Responding to the Death of a Student Member of the University policy (AC1215).

12.00 To locate the student's emergency contact or next-of-kin information, the staff or faculty member will determine if an emergency contact has been provided and will inform the respective department Chair or Director of the request for information and the need to check for the emergency contact. If the staff member does not have access to Banner, he or she may obtain assistance from the departmental or unit staff member with Banner access.

Disclosure of Personal Information in Compelling Circumstances

13.00 When a university faculty or staff member is faced with circumstances where the normal consent and other routes authorized by statute for disclosure are not available and where Compelling Circumstances exist:

(a) The faculty or staff member will consult with the department Chair, unit Director, or Dean;

(b) If urgent action is required, considering the nature of the circumstances and the obligations and protections under FIPPA and the university's Protection of Privacy

Policy (GV0235), the faculty or staff member and the appropriate department Chair, Dean or unit Director will jointly:

- review whether the disclosure should be made, to whom the disclosure should be made, and the content of the disclosure;
- make recommendations to one of the individuals listed in (d) below who is authorized to decide to disclose the Personal Information; and

(c) If time permits, the reviewing employee(s) may consult with counselling services, health services, or campus security as required.

When consulting with other units, the reviewing employee(s) shall only provide identifying Personal Information if the unit they are consulting with requests or requires it.

If the reviewing employee(s) transfers the responsibility for handling the matter to another university staff or faculty member, the reviewing employee(s) shall ensure that the staff or faculty member to whom the matter is being transferred is fully aware that they are now responsible for the matter.

(d) Where the recommendation is to disclose Personal Information about the student to an external agency, and the staff or faculty member has not yet contacted the Dean, the staff or faculty member shall contact one of the following individuals (or their designates) who will determine whether to authorize the disclosure of Personal Information:

i) The respective Dean or University Librarian, or where an incident occurs in a non-academic context (e.g., student housing) the Associate Vice-President Student Affairs (or designate);
   - The Dean or University Librarian will consult with the office of the Associate Vice-President Student Affairs (or designate) prior to determining whether to authorize the disclosure;

ii) If the Dean or University Librarian is not available, contact the Associate Vice-President Student Affairs (or designate) directly;

iii) If the Associate Vice-President Student Affairs is not available, contact the Director of Counselling Services or the Head of Health Services;

iv) If the individuals listed in iii) are not available, contact the General Counsel;

v) If the incident occurs after business hours, contact the individual on duty at Campus Security.

Record Keeping

14.00 The individual authorizing the disclosure under section 13.00 (d) above will maintain a confidential file containing a brief record of the disclosure decision and, a decision to assume the responsibility.

Notification

15.00 The individual authorizing the disclosure in Compelling Circumstances under section 13.00(d), is responsible to ensure, where appropriate, the student is notified in writing.

RELEVANT LEGISLATION

University Act
Freedom of Information and Protection of Privacy Act

RELATED POLICIES AND DOCUMENTS

Protection of Privacy Policy (GV0235)

- Procedures for the Management of Personal Information
- Procedures for the Management of University Surveillance Systems
- Procedures for Responding to a Privacy Incident or Privacy Breach

Records Management Policy (IM7700)

- Procedures for the Management of University Records
- Procedures for Access to and Correction of Information
- Guidelines for the Secure Destruction and Deletion of University Records and Information

Critical Incident Response Procedures (SS9115)
Responding to the Death of a Student Member of the University Policy (AC1215)
Violence and Threatening Behaviour Policy (SS9105)

University of Victoria

PROCEDURES FOR THE MANAGEMENT OF PERSONAL INFORMATION

Procedural Authority: President
Procedural Officer: General Counsel
Parent Policy: Protection of Privacy Policy (GV0235)

Effective Date: June, 2017
Supersedes: January, 2010
Last Editorial Change: July 2018

PURPOSE

1.00 The purpose of these procedures is to ensure that Personal Information in the custody or under the control of the university is managed in a manner that complies with the *Freedom of Information and Protection of Privacy Act* (FIPPA), and is consistent with the university's Protection of Privacy (GV0235), Records Management (IM7700) and Information Security (IM7800) policies and associated procedures.

DEFINITIONS

2.00 The definitions contained within the university's Protection of Privacy policy (GV0235) apply to these procedures.

3.00 Disclose means to transmit or provide, intentionally or unintentionally, Personal Information by any means to someone other than an Employee.

4.00 Use of Personal Information means employing or handling Personal Information by Employees to accomplish the university's objectives; for example, to:

- administer a program or activity;
- provide a service; or
- determine someone's eligibility for a benefit or suitability for a job.

PROCEDURES

5.00 The Privacy and Access Office's contact information will be provided for questions regarding the collection of Personal Information where the university provides notice of the collection of Personal Information.

6.00 Employees are responsible for consulting as necessary with the appropriate Administrative Authority or manager about the collection of Personal Information, the access and use of Personal Information, the disclosure of Personal Information to a third party, or the safeguarding of Personal Information.

Where an Employee has consulted the appropriate Administrative Authority or manager, that individual may contact the Privacy and Access Office for guidance on whether to permit the collection, the access or use by another Employee or the disclosure to a third party or the safeguarding of Personal Information.

Collection of Personal Information – Identifying Purposes, Limiting Collection and Consent

7.00 The university collects Personal Information related directly to and required by it to:

- fulfill its mandate under the *University Act*;
- carry out its operations and provide services; and
- generally to undertake activities related to the management of a post-secondary institution.

Specific types of student, faculty, staff, donor, and alumni Personal Information are collected for purposes including, but not limited to those listed in Schedule "A".

8.00 The university collects the Personal Information of:

- prospective and current students;
- prospective and current faculty and staff;
- alumni;
- prospective and current donors; and
- others (e.g., adjunct faculty, post doctoral, grant-funded personnel, volunteers, service providers, retirees)

through a variety of means, including but not limited to: in person, websites, telephone conversations and forms.

9.00 The university collects Personal Information in accordance with:

- FIPPA, the *University Act* and other applicable legislation authorizing collection;
- applicable university policies [including but not limited to the Protection of Privacy (GV0235), Records Management (IM7700) and Information Security (IM7800) policies];
- collective agreements; and
- other contracts.

10.00 Where the university collects Personal Information directly from an individual, and notice of the collection is provided at the time of collection, the individual's consent is implied.

10.01 Providing notice of collection means telling the individual the purpose of collection, legal authority for collection and the contact information of the person who can answer an individual's questions about collection.

11.00 In addition to collecting Personal Information for its own purposes, the university collects specific and limited Personal Information on behalf of student societies as permitted by the *University Act*.

11.01 Where required, appropriate consent for such collection, use and disclosure will be obtained by the university prior to such Personal Information being disclosed to student societies.

Use and Disclosure of Personal Information

Use of Personal Information – General

12.00 University Employees, including faculty or staff members may access and Use Personal Information, on a need to know basis, for a purpose:

- listed in sections 7.00, 11.00 or Schedule "A";
- that has a reasonable and direct connection to a purpose listed in sections 7.00, 11.00 or Schedule "A" and is necessary for faculty and staff members as part of their professional or university duties including the effective and efficient management of the university;
- for which the individual that the information is about has consented; or
- for which that information may be disclosed to the university by another public body under sections 33 to 36 of the FIPPA.

13.00 An Administrative Authority, responsible for authorizing Employee access to Personal Information in any media must only provide that authorization when access is required for a purpose listed in section 12.00. Authorized access should be sufficient that Employees can carry out their duties effectively and efficiently.

14.00 When there is a change to an Employee's position or duties, the Administrative Authority must review, and if necessary change, the Employee's authorized access to Personal Information in relation to job function changes in order to ensure that access to Personal Information is at a level and to an extent appropriate.

15.00 Faculty, staff, student, donor and alumni address information may be used for university mailing purposes only and will be used only for alumni/donor or university related functions.

16.00 Faculty, staff, student, donor and alumni Personal Information, including student Personal Information on admission, registration and academic achievement may be used for statistical and research purposes by the university in order to fulfil its mandate under the *University Act*.

16.01 Such information may also be used for other research purposes but in those cases individual identities will be removed.

17.00 In accordance with the university's Policy on Internal Audit (GV0220), the university's Chief Audit Executive, staff and agents of the Internal Audit department may use and access Records containing Personal Information in the custody or under the control of the university and relevant to the subject under review. This use and access is limited to the minimum amount of Personal Information necessary to meet Internal Audit's requirements.

Use of Donor and Alumni Information

18.00 Donor and alumni information may be used by select units within the university for approved university programs and activities as set out in below.

18.01 Donor and alumni Personal Information may be used by university units for mailings or publications, invitations to gatherings, fundraising and other university approved purposes.

18.02 Alumni Personal Information may be used by the Alumni Relations to offer Alumni Association benefits and services to alumni.

19.00 Requests for donor or alumni Personal Information from university units must be submitted to the Associate Vice-President Alumni and Development (or designate) who will review the request and consult with other senior administrators where required to ensure that the information requested is intended for an appropriate use and is necessary as part of the requestor's university duties. The Associate Vice-President Alumni and Development (or designate), may request clarification on the intended use to ensure that the purpose is in the best interest of the university, while protecting the privacy of alumni and donors.

Use of Student Personal Information

20.00 Faculty members who need to access student academic information, such as faculty advisors or members of admissions committees, will be granted access to that information through the individual authorized by the Administrative Authority to determine access to perform these job requirements.

21.00 Student grades (for term work or first term results in a full year coursework) may be posted providing that each student is identified by an incomplete or obscured student identification number or where code names are used. Incomplete or obscured identification numbers must be listed in random order (i.e., not in alphabetical order). Grades will not be posted for classes with ten or fewer students, as there is a possibility that students may be easily identified.

21.01 Section 21.00 applies to all methods of posting grades, including but not limited to:

- Lists placed in public areas;
- Online learning tools;
- Course websites; and
- Course e-mail lists.

22.00 Except where students have consented otherwise, student assignments and examinations must be returned directly to the student or left for general pick-up in the respective department office and not in a public area.

22.01 Faculty or staff may release assignments or examinations to a third-party where written permission, including by electronic means, has been provided in advance by the student authorizing a specific individual to pick up or receive the assignment or examination.

23.00 Class registration lists and photographs of students may be provided to faculty for teaching purposes and such information may only be Disclosed to other students in the class with the permission of the student and must not be posted in public places.

24.00 Information containing a student's address or phone number(s) may be provided to an instructor who is teaching the student or to a counsellor if the information is necessary for the performance of that individual's duties.

25.00 Access to and use of records of violations of academic integrity, are governed by the Policy on Academic Integrity as set out in the academic calendar.

26.00 Personal Information collected as a result of a request for academic concession is used only by the student's instructor(s) and other persons at the university whose involvement is required in the adjudication of the request for academic concession and only for the purpose of adjudicating the claim.

27.00 Faculty access to student comments compiled as part of the Course Experience Survey (CES) is provided after the grades are finalized, and the CES ratings are available through secure online access. Individual instructor evaluation data from the CES is available to administrators and committees responsible for tenure, promotion, annual review, or other purposes under the Faculty Collective Agreement. Student comments are made available for review of teaching performance only with permission from the faculty member. When a faculty member gives such permission all comments must be included. Aggregate data is available through the Office of the Vice-President Academic and Provost for the purpose of academic program quality review and assurance.

Disclosure of Personal Information (General)

28.00 Student, faculty, staff, donor, and alumni Personal Information will be disclosed only for a purpose authorized in the FIPPA, the university Protection of Privacy Policy or this procedure.

29.00 Unless specified below, requests from third-parties for disclosure of Personal Information must be made in writing, identifying the information sought, the authority for the request, and the reason for the request.

30.00 Specific records or portions thereof may be disclosed to persons or agencies where disclosure is required or authorized by an enactment of British Columbia or Canada.

This includes but is not limited to disclosure:

- in response to a court order, summons, or subpoena;
- in response to government agencies who demonstrate their authority to require or authorize disclosure in the circumstances in which they are requesting the information;
- in accordance with the statutory requirements of professional governing bodies for the purposes of licensing, registration, investigation and discipline of regulated persons; and

- to external auditors, engaged by the university who may access Personal Information collected by the university for auditing purposes.

31.00 Requests for disclosure of student, faculty or staff Personal Information from specific third parties will be treated as follows:

- Law Enforcement Agency Requests – refer the request to Campus Security.
- Media Requests - refer the request to UVic Communication Services.
- Lawyer and Insurance Company Requests - must be made in writing and be accompanied with the written consent for the release from the student, faculty or staff member.

32.00 Disclosure of student Personal Information by the university in emergency or compelling circumstances is described in the Procedures for the Disclosure of Student Personal Information in Emergency or Compelling Circumstances.

33.00 Where any individual is asked (a "Referee"), in the performance of a university function, to supply in confidence an assessment of student, faculty or staff, the assessment is considered to be supplied in confidence, unless the Referee expressly stated otherwise.

34.00 Subject to 34.01, 35.00 and 35.01, the university may enter a contract in which Personal Information is collected, used, accessed, disclosed, retained, stored or maintained only where the Personal Information is stored in and accessed in Canada.

34.01 The university may enter a contract where the contract proposes that Personal Information is stored or accessed outside of Canada, if the contract provides that the written consent of the individual student(s), staff or faculty is obtained. Such consent must be obtained in the manner prescribed under the FIPPA regulation.

35.00 The university may Disclose Personal Information outside of Canada where it is necessary for installing, implementing, maintaining, repairing, trouble-shooting or upgrading an electronic system or equipment or for data recovery following the failure of the electronic system. In this case the university is not required to obtain explicit consent.

35.01 The Disclosure of Personal Information outside of Canada must be limited to temporary access and storage for the minimum time necessary for the purpose in 35.00. In the case of data recovery, Disclosure is limited to access and storage only after the system failure has occurred.

35.02 Disclosure under sections 35.00 and 35.01 must be done in a manner prescribed by the Chief Information Officer or designate.

36.00 Where the university is requested by a third party to Disclose Personal Information outside of Canada, the university will seek the written consent of the individual student, staff or faculty, unless otherwise permitted by FIPPA. Such consent must be obtained in the manner prescribed under the FIPPA regulation.

37.00 Faculty or staff who wish to conduct surveys, including electronic that collect Personal Information in identifiable form must, where appropriate, obtain approval from the relevant ethics review body, and use a Canadian based service provider that stores the information in Canada, or must obtain the consent of each individual completing the survey to have their Personal Information stored outside of Canada. Such consent must be obtained in the manner prescribed under the FIPPA regulation.

38.00 The university may Disclose Personal Information to external bodies for accreditation purposes.

38.01 Units shall make reasonable efforts to remove all individual identifiers before Disclosing the information to the accreditors.

38.02 If the accreditors are not able to view the Personal Information on site, the accreditors shall make reasonable arrangements for the secure transmission within Canada of the records containing Personal Information and secure return or disposal of any copies of the records provided.

Disclosure of Student Personal Information

39.00 The university may Disclose, without consent, the student's or former student's name, name of degree, diploma and certificate, and the year the award was granted.

39.01 The Disclosure of such information may be restricted or delayed in specific cases for security or other legitimate reasons.

40.00 Except for the circumstances in sections 30.00 and 32.00, Disclosure of student Personal Information (e.g., attendance, academic progress, grades, payments, fees, class schedule, enrollment, course selection) to a third party, such as a relative, employer, funding agency, legal process server or sponsor is permitted only with the student's consent.

41.00 The university may Disclose graduating student's information to third parties, such as photography studios, only through specific contracts.

42.00 Disclosure of Personal Information beyond that listed in 39.00 to another university, post-secondary institution, professional governing body or potential employer requires the consent of the student or former student. If the student has not previously provided consent, consent must be obtained before Disclosing Personal Information.

42.01 Where a student or former student requests a reference, consent for the Disclosure of all relevant and necessary Personal Information is implied.

43.00 Student Personal Information may be Disclosed to a donor for the purpose of notifying the donor of the granting of an award or scholarship. In such cases, the university will provide notice to students.

Disclosure of Faculty or Staff Personal Information

44.00 The university may Disclose without consent the following Personal Information about a current or former staff or faculty member:

- information about an individual's position, function, or total remuneration as an officer, Employee, or member of the university; or
- their business contact information.

44.01 Requests for remuneration information shall be referred to HRIS/Payroll.

44.02 Disclosure under s. 44.00 does not include information about discretionary benefits/bonuses.

45.00 Disclosure of Personal Information beyond that listed in 44.00 to a potential employer requires the Employee's consent. If the Employee has not previously provided consent, consent must be obtained before disclosing Personal Information to the potential employer.

45.01 Where an Employee or former Employee requests a reference, consent for the Disclosure of all relevant and necessary Personal Information is implied.

46.00 University Employees will ensure that their curriculum vitae or resume does not contain Personal Information that the individual does not wish to Disclose and does not contain the Personal Information of others, without their consent.

47.00 Employee Personal Information may be Disclosed where the Disclosure is in accordance with the provision of a collective agreement authorizing or requiring the Disclosure.

Disclosure of Donor and Alumni Personal Information

48.00 Except as provided in sections 48.01 and 49.00, donor names and donation amounts will only be disclosed with the consent of the donor, or where disclosure is required by law.

48.01 On an annual basis, the university may publish names of donors listed by contribution category. Donors may choose to be listed as anonymous.

49.00 Donor Personal Information may be Disclosed to the University of Victoria Foundation or the Foundation for the University of Victoria.

50.00 Alumni Personal Information may be Disclosed to the Alumni Association, including its volunteers, for the purpose of carrying out the joint objectives of the university and the Alumni Association through alumni engagement programs and activities.

Accuracy of Personal Information

51.00 The university is committed to ensuring the accuracy of the Personal Information in its custody or under its control. Procedures for the correction of Personal Information are contained within the university's Procedures for Access to and Correction of Information.

Safeguarding Personal Information

52.00 Any individual or committee member making a decision or recommendation, including a decision or recommendation on any of the following matters:

- hiring, termination, and managing the employment relationship;
- search, selection and appointment;
- employment accommodation;
- academic accommodation;
- academic concession;
- renewal, reappointment, tenure or promotion;
- admission to the university or to a program or faculty within the university and associated matters;
- evaluation of academic or employment performance;
- awards or honours;
- investigation of complaints or allegation of misconduct (including but not limited to allegations of violence or threatening behaviour, discrimination or harassment);
- imposition of discipline;
- confidential consultations under the university's Discrimination and Harassment Policy (GV0205);
- handling of informal complaints received in confidence but not investigated or an environmental assessment under the university's Discrimination and Harassment Policy (GV0205) and its related procedures; or
- faculty or staff member's disclosure of conflict of interest

must treat the Personal Information of any individuals created, submitted, considered or investigated during that process as confidential in accordance with the university's Protection of Privacy Policy (GV0235) and other provisions of this procedure.

52.01 Individuals responsible for a process under section 52.00, or where appropriate committee members covered under section 52.00 must make reasonable efforts to safeguard the Personal Information created or received by:

- ensuring, unless to do so would jeopardize a process under section 52.00, there is a clear statement of the purpose of the collection and that the Personal Information will only be used or Disclosed for the original purpose for which it was collected or for a purpose consistent with the original collection purpose;
    - this statement may be by means of a collective agreement or university policy or procedure;
- specifying who, other than the individual or committee under section 52.00, may have access to the Personal Information and under what circumstances;
- describing how the Personal Information will be circulated and retained;
- marking the records as confidential prior to any permissible Disclosure;

- taking reasonable security measures to ensure the security of the record, such as storage in locked cabinets or protection of electronic files; and
- maintaining, retaining and destroying the record, in accordance with the university's Records Management policy and related procedures, the University Information Security Classification Procedures (Under Development), and the Directory of Records.

53.00 Medical information, including counselling information, created, submitted, or considered as part of the university responding to a request for service shall be treated as confidential in accordance with the university's Protection of Privacy Policy and other provisions of this procedure and the procedures outlined in section 52.01 shall be followed.

54.00 Unless otherwise provided in a collective agreement, personnel and labour relations information, including grievance or appeal information created, submitted or considered as part of the university responding to a labour relations matter or a grievance shall be treated as confidential in accordance with the university's Protection of Privacy Policy (GV0235) and other provisions of this procedure and the procedures outlined in section 52.01 shall be followed.

55.00 An individual or committee is not precluded from Disclosing Personal Information that is being Disclosed for a purpose:

- consistent with the purpose for which it was collected, compiled, or used;
- permitted by law;
- permitted under a collective agreement; or
- required as part of a review by the university's Chief Audit Executive or an audit required by law, contract, or university policy.

56.00 A claim of confidentiality may be made where the record is part of a series of confidential communications. Confidentiality may be implied from the circumstances (including those listed in 52.01) surrounding the creation and treatment of the record.

57.00 When the university enters into or modifies an agreement with an external organization to undertake work on its behalf (including third-parties processing mail-outs for university purposes) that involves the collection, use or Disclosure of Personal Information, the university will attach the Privacy Protection Schedule to the agreement or contract to ensure that the third-party treats the Personal Information in accordance with FIPPA and the university's Protection of Privacy policy and its associated procedures. Such arrangements must include secure transmission and secure and timely destruction or return.

57.01 A contract that is amended or assigned must continue to comply with the Protection of Privacy Policy and its associated procedures.

57.02 In exceptional circumstances the General Counsel (or designate) may waive the requirement in section 57.00 where the external organization has provided a

written undertaking that its policies and practices are consistent with the requirements of FIPPA.

Individual Access to Personal Information

58.00 The university's Access to and Correction of Information procedure addresses access to Personal Information access requests.

RELEVANT LEGISLATION

University Act
Freedom of Information and Protection of Privacy Act

RELATED POLICIES AND DOCUMENTS

Academic Calendar

Protection of Privacy Policy (GV0235)

- Procedures for the Disclosure of Personal Information in Emergencies and Compelling Circumstances
- Procedures for the Management of University Surveillance Systems
- Procedures for Responding to a Privacy Incident or Privacy Breach
- Procedures for Responding to the Loss or Theft of a Mobile Computing Devices
- University Information Security Classification Procedures
- Privacy Protection Schedule

Records Management Policy (IM7700)

- Procedures for the Management of University Records
- Procedures for the Access to of Correction of Information
- Guidelines for the Secure Destruction and Deletion of University Records and Information

Information Security Policy (IM7800)

- Procedures for Responding to an Information Security Incident

University of Victoria

SCHEDULE "A" – UNIVERSITY PERSONAL INFORMATION TYPES AND COLLECTION PURPOSES

PURPOSE: The purpose of this Schedule is to set out **examples** of the types of Personal Information the University collects and the purposes for such collection.

Categories of Individuals	Personal Information Types	Collection Purposes
Students	**Identity-Related Information** • Name • Address • Telephone number(s) • Personal Education Number • Birth date • Gender **Related Academic Information** • Previous education • Programs of study • Performance information • Degrees, diplomas, and certificates obtained **Related Financial Information** • Charges • Payments **Related Fiscal Information** • Social Insurance Number • Tuition fees • Bursaries Citizenship and immigration status **Related to responding to request for services** • Medical information	• Confirmation of identity • Identification of university documents • Recruitment, admission, registration, reregistration and graduation • Provision of student awards and funding; • Recording academic progress and achievement • Advising • Issuance of transit and parking passes; • Provision of computing and e-mail accounts • Communication with students • Administration and operation of academic, library, athletic, recreational, residences, alumni and other university programs • Administration and management of the use of university information and communication systems • Assessment of fees • Assessment of medical premiums • Completion of taxation and tax deduction forms • Assessment of eligibility for TOEFL waiver • Evaluating employment applications and making hiring decisions • Management of the university's financial affairs

		• Responding to an emergency or urgent circumstance • Provision of targeted services to a defined student group
Faculty and Staff	**Identity-Related Information** • Name • Address • Telephone number(s) • Birth date • Gender • Citizenship **Related Financial Information** • Payments • Donations **Related Fiscal Information** • Social Insurance Number **Related Employment Equity Information** • Disability status • Aboriginal status • Visible minority status **Related employment information** • Employment history • Credentials **Related to responding to request for services** • Medical information	• Evaluating employment applications and making hiring decisions • Administration of payroll and benefits; • Evaluating performance for reappointment, tenure and promotion • Research funding • Selecting graduate students • Issuing of parking passes • Creation of computing and e-mail accounts • Registration for recreational and other university services • Conducting investigations and making disciplinary and termination decisions • Complying with requirements of the Federal Contractors Program • Administration and managing the use of university information and communication systems • Business Continuity • Disclosure for conflict of interest purposes
Donor and Alumni	**Identity-Related Information** • Name, including spouse and children • Family or marital status • Address(es) • Telephone number(s)	• Recording and receipting donations; • Fundraising • Community relations

Donor and Alumni 'Continued'	• Birth date, including spouse and children **Related financial information** • Pledges and donations • Personal financial history • Professional history **Related Alumni/Donor information** • Involvement in events and activities • Hometown, interests, photograph, and education	• Building relationships between the university and its constituencies, including engaging alumni.

University of Victoria

UNIVERSITY INFORMATION SECURITY CLASSIFICATION PROCEDURES

Procedural Authority: Vice-President Finance and Operations
Procedural Officer: Chief Information Officer

Parent Policies: Information Security Policy (IM7800)
Protection of Privacy Policy (GV0235)

Effective Date: January, 2015
Supersedes: December, 2010
Last Editorial Change: June, 2017

PURPOSE

1.00 The purpose of these procedures is to set out the minimum standards necessary for classifying various types of university Information Resources so that reasonable security arrangements can be applied to such information.

DEFINITIONS

2.00 The definitions contained within the university's Information Security (IM7800) and Protection of Privacy (GV0235) policies apply to these procedures.

Note: Refer to the Procedures for the Management of University Records and the Directory of Records for information on the functional classification of university Records. Refer to the Procedures for the Access to and Correction of Personal Information for information regarding freedom of information access requests.

See Section 8.00 for definitions of security classification levels.

PROCEDURES

Assigning an Information Security Classification Level

3.00 Information Resources require security classification at the level appropriate for that resource, in accordance with the classification levels set out in section 8.00.

3.01 The security classification level of the Information Resource establishes the extent and type of security arrangements that must be implemented in order to protect the Information Resource.

3.02 Prior to assigning a security classification level, Units must be aware of relevant legislative requirements and regulatory obligations, and relevant university policies and procedures. Units may also refer to industry standards and best practices for further direction where applicable.

4.00 Administrative Authorities are expected to classify and manage the Information Resources for which they are responsible based on a reasonable understanding of the overall value of the Information Resource. Where appropriate, Administrative Authorities should collaborate with Providers and University Archives to classify and manage the Information Resources for which they are responsible.

5.00 Administrative Authorities are expected to ensure that Users in their Units manage Information Resources according to the assigned security classification.

6.00 Security classification levels are applied to broad information types or categories, rather than individual records.

7.00 Where it is unclear which security classification level is most appropriate or when dealing with large volumes of information, Units should employ the highest appropriate classification level.

7.01 Where an Information System or Record contains information that is classified as public and information classified at a higher level, the combined information must be managed at the higher confidentiality level.

7.02 In deciding which security classification level is most appropriate, units will take into account the volume of information and should consider employing a higher classification level. An increase in risk due to volume may necessitate using a higher security classification level.

Information Classification Levels

8.00 University Information Resources are classified according to the classification levels in the following chart.

	Highly Confidential	Confidential	Internal	Public
Definition	Information Resource is so sensitive or critical that it is entitled to extraordinary protections, as defined in 9.00.	Information Resource is considered to be highly sensitive business or Personal Information, or a critical system. It is intended for a very specific use and may not be disclosed except to those who have explicit authorization to review such information, even within a workgroup or Unit.	Information that is intended for use within the University or within a specific workgroup, Unit or group of individuals with a legitimate need-to-know. Internal Information is not approved for general circulation outside the workgroup or Unit.	Information that has been approved for distribution to the public by the information owner or Administrative Authority or through some other valid authority such as legislation or policy.
Legal Requirement	Protection of information where it is required by law or regulation (e.g. FIPPA or PCI-DSS), or as determined by contractual obligation.	The University has a contractual or legal obligation to protect the information.	The University has a contractual obligation to protect the information.	Information may be mandated by legislation (e.g. FIPPA) to be public information.
Reputational Risk	Critical loss of trust/credibility. Significant media attention. Business unit will be subject to special training and processes.	Significant loss of trust/credibility. Guaranteed to generate media attention and increased scrutiny.	Potential for lost trust/credibility. May generate some media attention and result in increased scrutiny.	No impact on reputation.
Operational Risk	Risk will render the business unit unable to achieve its overall objectives or mandate.	Significant impact on business unit's ability to achieve its objectives.	Moderately impacts business unit's ability to achieve its objectives.	Little or no impact on the business unit's ability to achieve its objectives.
Financial Risk	Major revenue loss, or impact on business unit budget, including research funding, or fines.	Significant revenue loss, or impact on business unit budget, including research funding, or fines.	Minor negative financial impact for the business unit.	Impact is within normal operating budget margin fluctuations.
Disclosure Risk	Highly-adverse negative impact on the university, individuals or affiliates, including identity theft.	Moderately-adverse negative impact on the university, individuals or affiliates, including identity theft.	Possible adverse impact on the University, individuals or affiliates.	Disclosure of public information requires no further authorization and may be freely disseminated without potential harm to the University or its affiliates.

8.01 **Prohibited Information:** In addition to the above classification levels, certain information may be deemed by industry regulations, legislation, or other mechanism to be Prohibited. Such information may not be collected or stored by the University in any form.

Security Arrangements for Classification

9.00 After an Information Security Classification has been applied, reasonable security arrangements are required that correspond to the assigned classification level. The following table sets out appropriate safeguards for each level of information.

	Highly Confidential	Confidential	Internal	Public
Access	• Access is limited to specific named individuals or positions. • Principles of least-privilege and need-to-know must be applied • Access must be revoked immediately when users leave the university or the custodial Unit.	• Access is limited to individuals in a specific function, group, or role. • Principles of least-privilege and need-to-know must be applied • Access must be revoked as soon as reasonably possible when Users leave the university or the custodial Unit.	• Access is limited to employees and other authorized Users for business-related purposes. • Access must be revoked as soon as reasonably possible when Users leave the university or the custodial Unit.	• No access restrictions
Transmission	• Encryption for public networks (e.g. wireless, Internet). • Encryption strongly-recommended on trusted, internal networks. • Third-party email providers are not appropriate for transmitting. • Data may be masked instead of encrypting. • Double envelope mailings for hardcopy records	• Encryption for public networks (e.g. wireless, Internet). • Encryption strongly recommended on trusted, internal networks. • Third-party email providers are not appropriate for transmitting. • Data may be masked instead of encrypting. • Clearly marked “confidential” on sealed mailings.	• Encryption strongly recommended on public networks (e.g. wireless, Internet)	• No special handling required.
Storage	• Stored within a controlled-access system (e.g., password protected file or file system, locked file cabinet, alarmed area). Additional controls implemented as necessary to comply with relevant legislation or other requirements. • Encryption mandatory on mobile devices and workstations, and	• Stored within a controlled-access system (e.g., password protected file or file system, locked file cabinet, alarmed area). • Encryption mandatory on mobile devices and workstations, and strongly-recommended in all environments • Implement “clean desk” policy • Must be stored in Canada	• Stored within a controlled-access system (e.g., password protected file or file system, locked file cabinet). • Encryption strongly recommended in all environments.	• No special safeguards required.

	strongly recommended in all environments. • Implement “clean desk” policy • Must be stored in Canada			
Destruction	• Shredded or erased in accordance with the university’s Guidelines for the Secure Destruction of Information	• Shredded or erased in accordance with the university’s Guidelines for the Secure Destruction of Information	• Shredded or erased in accordance with the university’s Guidelines for the Secure Destruction of Information	• Recycle

RELEVANT LEGISLATION

Freedom of Information and Protection of Privacy Act

RELATED POLICIES AND DOCUMENTS

Information Security Policy (IM7800)

Procedures for Responding to an Information Security Incident

Protection of Privacy Policy (GV0235)

Procedures for Responding to a Privacy Incident or Privacy Breach

Procedures for the Management of Personal Information

Procedures for the Management of University Surveillance Systems

Records Management Policy (IM7700)

Procedures for the Access to and Correction of Information

Procedures for the Management of University Records

Guidelines for the Secure Destruction and Deletion of University Records and Information

Responsible Use of Information Technology Resources (IM7200)

APPENDIX A: INFORMATION CLASSIFICATION EXAMPLES

The following chart provides examples of the types of information and their security classification.

	Example
Public	• Annual reports • Advertising and media releases • Product and service information • Employee directory listings • Academic calendar • Published research presentations or papers • Job postings • Training manuals • Open-session Board and Senate minutes • Name of degree, diploma and certificate recipients • Campus maps
Internal	• Budget information • Personal pager or cell phone numbers • Select Unit procedures • Student Number (V-number) • Student Grades (including test scores, assignments, and class grades) • Employee V-number
Confidential	*Enrolled and Prospective Student Data* • Social Insurance Number • Driver's License Number • Student financials (bank accounts, wire transfers, payment history, financial aid/grants) • Biometric identifiers, including finger and voice prints, and full face images • Personal vehicle information (serial numbers, license plate number) • Access device numbers (ISO number, building access code, keys, etc.) • Reference Letters • Information protected by non-disclosure agreements • Any other unique identifying number, characteristic, or codes • Payment Guarantor's and beneficiary information • Student contact or class lists • Enrolment status of an individual *Employee Information* • Social Insurance Number • Personnel Files • Personal vehicle information (serial numbers, license plate number) • Accounting information (tax records, employee payroll, staff loans, etc.) • Access device numbers (ISO number, building access code, keys, etc.)

	• Biometric identifiers, including finger and voice prints, and full face images • Information protected by non-disclosure agreements • Personal financial information, including non-UVic income level and sources • Insurance benefit, payment guarantor's and beneficiary information • Pension records • Employee demographic information • Any other unique identifying number, characteristic, or code • Home/Personal address, phone number, cell number, email address *Donor/Alumni Information* • Donor's Name • Social Insurance Number • Personal financial information • Donor Profile (personal & family history) • Bank account numbers, amount donated • Telephone/fax numbers, email address • Information protected by non-disclosure agreements • Any other unique identifying number, characteristic, or code *Research Information* • Research Information (Granting Agency Agreements, Other IRB Governance) • Sensitive research data *Business/Vendor Data* • Contract information (between UVic and a third party) • Access device numbers (building access code, etc.) • Biometric identifiers • Certificate/licence numbers, device IDs and serial numbers, email, URLs, IP addresses *Other Institutional Data* • Confidential Information in Contracts • Physical plant detail • Critical infrastructure detail • User account passwords
Highly-Confidential	• Legal suits • Closed or In camera Board of Governors or Senate documents • Academic concessions • Appeals, and grievances • Criminal records checks • Health, disability or counselling information • Harassment and discrimination reports • Authentication credentials • Personally-identifiable research information

Prohibited	*Credit Card Data / Payment Card Industry Data Security Standard (PCI DSS) (when taken as part of a financial transaction)* • Service Code • ISO Number • CVC2, CVV2 or CID value • PIN or PIN block • Contents of a credit card's magnetic stripe (specifically "Track 2" data)

University of Victoria

PROCEDURES FOR RESPONDING TO THE LOSS OR THEFT OF A MOBILE COMPUTING DEVICE

Procedural Authorities: Vice-President Finance and Operations; General Counsel
Procedural Officer: Chief Information Officer; General Counsel
Parent Policies: Information Security Policy (IM7800); Protection of Privacy Policy (GV0235)

Effective Date: December, 2010
Supersedes: NEW
Last Editorial Change: July 2018

PURPOSE

1.00 The purpose of this document is to set out response procedures in the event of the loss or theft of a university Mobile Computing Device in order to protect the information contained on the device.

DEFINITIONS

2.00 The definitions contained within the university's Protection of Privacy and Information Security policies apply to these procedures.

3.00 **Mobile Computing Device** means any portable device that provides computing or information storage and retrieval including but not limited to: laptop computers, Personal Digital Assistants (PDA), cell phones, smart phones, flash drives, video cameras, compact disks (CD), digital video disks (DVD), and portable hard drives.

PROCEDURES

User Responsibility

4.00 Users of university Mobile Computing Devices are expected to make reasonable security arrangements to protect such devices from loss or theft and to protect information stored on such devices.

Identification and Reporting

5.00 Loss or theft of a university Mobile Computing Device must be immediately reported to Campus Security and to the Unit's Administrative Authority.

5.01 When reporting the loss or theft, Users are expected to inform Campus Security of whether the Mobile Computing Device contains Personal Information, or information classified as Internal, Confidential or Highly Confidential under the university's Information Classification procedure.

6.00 Campus Security will conduct an initial assessment and create an incident report.

7.00 Campus Security shall immediately inform the Information Security Office if the lost or stolen Mobile Computing Device contains:
(a) Personal Information; or
(b) Internal, Confidential, or Highly-Confidential information (as defined in the University Information Security Classification procedures).

8.00 Where the Information Security Office confirms that the lost or stolen Mobile Computing Device contains Personal Information, the Information Security Office shall immediately contact the Privacy and Access Office.

Response

9.00 In cases where Personal Information is contained on a lost or stolen Mobile Computing Device, the General Counsel, where warranted, will follow the Procedures for Responding to a Privacy Incident or Privacy Breach.

9.01 Where the information contained on the Mobile Computing Device is non-personal and Internal, Confidential or Highly-Confidential, the Information Security Office, where warranted, will follow the Procedures for Responding to an Information Security Incident.

RELATED POLICIES AND DOCUMENTS

Protection of Privacy Policy (GV0235)
- Procedures for Responding to a Privacy Incident or Privacy Breach
- University Information Security Classification Procedures

Records Management Policy (IM7700)
- Procedures for the Management of University Records
- Procedures for Access to and Correction of Information
- Guidelines for the Secure Destruction and Deletion of University Records and Information

Information Security Policy (IM7800)
- University Information Security Classification Procedures
- Procedures for Responding to an Information Security Incident