



## **RESPONSIBLE USE OF INFORMATION TECHNOLOGY SERVICES**

**University Policy No.:** IM7200  
**Classification:** Information Management  
**Approving Authority:** Vice President  
Finance and Operations  
**Effective Date:** February/08  
**Supersedes:** April/86  
**Last Editorial Change:**  
**Mandated Review:**

### **1. Introduction**

Information technology services at the University of Victoria are intended primarily to serve the educational, research, and administrative purposes of the University. The University is therefore responsible for ensuring that resources and facilities provided for the purpose of supporting University-authorized teaching, research, administrative, and other University computing activities are in fact used for these purposes. Usage is also governed by all applicable University policies, such as the Harassment and Intellectual Property Policies, by all applicable Federal, Provincial, and local laws and statutes, such as the Criminal Code of Canada, the Copyright Act, and the BC Freedom of Information and Protection of Privacy Act, and by licenses governing the use of computer programs and documents of all kinds.

This is a University-wide policy pertaining to information technology services and to the resources these technologies make available in support of the University mission. It applies to all computing, communications, and networking resources connected to University facilities including:

- those owned by institutional agencies of the University;
- those owned by individual units such as faculties, departments/schools, or research groups;
- those owned by individuals when connected to or communicating with University information technology services.

This policy is applicable to all members of the University community when using any University computing, networking, or communication facilities, whether located at the University or elsewhere.

### **2. General Principles**

- 2.1 Each user of information technology services bears primary responsibility for her or his use of these services and for the information he or she transmits, receives, or stores through use of these services.
- 2.2 Incidental use of information technology services for personal use is acceptable but is limited to such responsible activity as minimizes disruption of University business while attending to necessary personal affairs.

- 2.3 Use of information technology services for commercial purposes is limited by University policies governing commercial activities sponsored by the University, for the purpose of enhancing the University's educational mission.
- 2.4 Connection of privately owned computer equipment to University communications services is permitted. Access to University information technology services from these computers, or from computers attached to remote networks, is also permitted. All such usage is governed by this policy.
- 2.5 Connection of privately owned communications equipment, with the intention of extending communications capabilities to other computer or communications equipment, is prohibited without specific authorization of the University.

### **3. Responsibilities**

As a condition of access to information technology services and facilities, a user agrees:

- 3.1 not to compromise or attempt to compromise the integrity of any computing or communications system;
- 3.2 not to use any computing or communications system or user account unless formally and explicitly authorized to do so;
- 3.3 not to misrepresent her or his identity as a sender of messages or the content of such messages;
- 3.4 not to seek by any means copies of or information regarding passwords, data, or programs of another user unless explicitly authorized to do so by that user;
- 3.5 not to harass other users of information technology services or facilities;
- 3.6 not to use any University information technology service or facility for non-University projects;
- 3.7 not to use any University information technology service or facility for commercial or other external purposes except as allowed by 2.3;
- 3.8 not to attempt to disrupt, degrade, or interfere with the normal operation of any information technology service or facility;
- 3.9 not to download or use unlicensed or unauthorized copies of computer software;
- 3.10 not to display or transmit information that violates Canadian laws (i.e., copyright, criminal code);
- 3.11 not to monitor network transmissions without authorization;
- 3.12 not to use a University computer account without authorization after an individual's relationship with the University has terminated;

- 3.13 to take all reasonable precautions to minimize opportunities for unauthorized persons to obtain access to passwords and files;
- 3.14 to be aware of computer viruses and other destructive programs and to take steps to avoid being a victim or unwitting carrier;
- 3.15 not to introduce or propagate any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer system, network, or communication facility.

The above clauses are representative examples and do not comprise a comprehensive list of unacceptable uses. Any exception to the above clauses must have the prior approval of the appropriate University authority.

#### **4. Abuse of Responsibilities**

Abuse or misuse of information technology services or facilities may not only be a violation of user responsibilities and applicable University policies but also of the Criminal Code of Canada. Such violations may include the input of textual or graphic materials that could reasonably be questioned as a violation of Criminal Code of Canada provisions respecting pornography.

In any circumstances of alleged abuse or misuse, formal procedures permit persons responsible for computing, networking, or electronic communications to request institutional authorization to examine directories, files, or other electronic records that are relevant to the investigation of the allegation.

- 4.1 An allegation of abuse shall be made to the Chair or Head of the unit or to the Officer who authorized access to the computing, networking, or communication services and facilities by the individual; this person shall be referred to as the investigating official throughout this policy.
- 4.2 The investigating official shall investigate any allegation in accordance with the rules of natural justice. The investigating official may elect to appoint an ad hoc committee if that is appropriate to ensure a fair review.
- 4.3 If the investigating official finds just cause, for example, that another individual or the integrity of the system is compromised, he or she shall have the right to suspend user privileges pending the outcome of that investigation.
- 4.4 If the matter relates to the Harassment Policy and Procedures, the investigating official shall refer the case to the Office for Prevention of Discrimination and Harassment for resolution. If the investigating official has suspended the user's privileges, this suspension shall remain in effect until the matter has been resolved.
- 4.5 If the investigating official deems it necessary when investigating the allegation, he or she shall designate a staff member to examine stored and printed data or to examine user files, programs, passwords, accounting information, printouts, and any other materials as enabled or permitted by law. The information so gathered shall be transmitted to the investigating official with an obligation to maintain the privacy of the user's data.

- 4.6 If the investigating official finds that abuses and/or misuse have taken place that may constitute grounds for discipline of an employee, then that discipline will be in accordance with the Framework Agreement or the appropriate Collective Agreement; and the investigating official will contact Human Resources.
- 4.7 If the investigating official finds that a student is responsible for abuses and/or misuse, he or she may apply one or more of the sanctions in paragraphs 4.7.1, 4.7.2, or 4.7.3 or may recommend as appropriate one or more of the sanctions in paragraphs 4.7.4, 4.7.5, or 4.7.6. The two groups of sanctions are NOT mutually exclusive.
  - 4.7.1 Dismissal of the allegation with a warning.
  - 4.7.2 A reprimand to be placed in the student's file.
  - 4.7.3 Discontinuance of computing or communications privileges.
  - 4.7.4 Other disciplinary action as deemed permissible.
  - 4.7.5 Suspension by the President from the University.
  - 4.7.6 Pursuit of whether charges may be laid under the Criminal Code of Canada.
  - 4.7.7 The regular University channels of appeal shall be available to the user in respect of the decision made by the investigating official.
  - 4.7.8 In the case where the user's privileges have been suspended and the allegation is dismissed, the user shall not suffer any academic penalty as a result of the suspension. However, the user shall not be entitled to reimbursement.

## **5. The Use of Electronic Mail (email)**

- 5.1 The University email system is part of the University's information technology services and is maintained for the purpose of carrying on the administration and business of the University. The email records created by using University computers or the University email system are University records and are, therefore, records for the purposes of the Freedom of Information and Protection of Privacy Act.
- 5.2 As indicated in Section 2, University information technology services are not to be used for non-University projects or commercial purposes. Nevertheless, as with the use of University telephones for local calls, occasional and limited use of email for personal purposes is permitted when it enables an employee to deal with personal matters. Abuse or misuse of email can however lead to the various sanctions previously outlined.
- 5.3 Email messages are University records that may be either transitory or required for ongoing purposes. If an email record is transitory, it should be disposed of when no longer required. Email deleted from the local computer is the equivalent of shredded records or records put in a recycling bin. Central back-up is not used for archival purposes (see section 5.5 below).
- 5.4 If a request for access is received under the Freedom of Information and Protection and Privacy Act, existing email records are included and must not be deleted.

- 5.5 Email, similar to other records containing personal information under the Freedom of Information and Protection of Privacy Act, can be reviewed by those in the University with a "need to know". This may relate to a request under the Freedom of Information and Protection of Privacy Act, labour relations issues, a reasonable suspicion of abuse of the email system, or the need for business access in the absence of an employee. Central back-up of email is for purposes of disaster only and not for recovery of specific items of deleted email for freedom of information access or other requests. There is not central back-up for archival purposes.
- 5.6 Outgoing email may be used by the recipient in a manner beyond the employee's control. Inappropriate or offensive email must not be sent or forwarded.
- 5.7 As email bears identification marks of University of Victoria, users are expected to treat email facilities in the same manner as they would use University letterhead.
- 5.8 Notwithstanding anything in this policy, the University reserves the right to access email records which have been deleted by an employee but which have been preserved centrally, for the purposes of recovering evidence while investigating allegations of serious employee misconduct and managing actual or potential civil litigation in which the University is or may become a party.

## **6. The Use of Broadcast Email**

- 6.1 Where the safety of university students, staff, faculty or visitors is considered to be at imminent risk, or where the demands of a critical incident on campus make it necessary, the director of campus security and the director of communications or their designates are authorized to arrange for the issuing of broadcast e-mail or other mass communications as they deem necessary in the circumstances. Where possible, they will seek the approval of the president or a vice-president of the university but, in all cases, they will advise members of Executive Council whenever their authority under this section has been exercised.
- 6.2 Other unsolicited email messages to all faculty, staff and/or students, or major segments thereof, may only be sent if the message is institutional in nature or relates to the critical operation of the university and permission has been granted by the university secretary, with the exception of emails authorized by the registrar and executive director, student enrolment under section 6.2.1.
  - 6.2.1 Messages for all students or specific student segments pertaining to critical academic business, or university-wide deadlines or schedules may be sent with permission from the registrar and executive director, student enrolment or designate.
  - 6.2.2 Messages from the UVSS or GSS to their members may be sent with permission from the university secretary.
- 6.3 These guidelines do not pertain to campus and other listservs that segments of the University community have knowingly joined.

## **7. General**

- 7.1 This policy shall be given to the user at the time access to computing and communications facilities is given. The user shall acknowledge understanding and compliance with this policy.
  - 7.2 A banner notice comprised of a brief summary of the policy shall be displayed when a user logs on to the system.
  - 7.3 The intellectual property provisions of copyright law are operative for all materials stored in electronic form. Unless the material is clearly in the public domain or unless there is explicit release by the copyright owner, information available on a computer network or the Internet may not be copied nor distributed without permission.
-