
APPROPRIATE USE OF COMPUTING AND NETWORK RESOURCES

AUTHORITY President
PRIMARY CONTACT Vice-President (Administration)
RELATED POLICIES

POLICY

The University of the Fraser Valley is committed to an intellectual environment in which students, faculty, and staff feel free to create, and to collaborate with colleagues, both at the university and elsewhere, without fear that the products of their intellectual efforts will be violated, misrepresented, tampered with, destroyed, or stolen. This environment is fostered by an atmosphere of trust and confidentiality. Therefore, UFV will provide computing and network resources with the fewest possible restrictions. Some restrictions on use are required, however, to protect the integrity of the resources, and these are explained below.

DEFINITIONS

Computing and Network Resources: Due to changes in technology, the components of computing and network resources are constantly changing. The list of University computing and network resources includes, but is not limited to, the following:

- Computers and peripherals attached to computers such as printers, plotters, scanners, cameras, fax machines, disk drives, and tape drives;
- Network hardware and peripherals attached to networks such as computers, printers, plotters, scanners, fax machines, disk drives, tape drives, and communication equipment used to electronically link computers, LANs, WANs or institutions together;
- All software, both system and application, that is used on computers, networks, and their peripherals;
- Information that is stored or generated on computers, networks, and their peripherals.

User(s): The computing and network resources of UFV are provided for the use of UFV faculty, staff, students, and in particular circumstances, the public (public use is restricted to the Libraries and Career Resource Centres). This group of users, UFV faculty, staff, and students, and in particular circumstances, the public, are authorized users of the computing and network resources at UFV. Hereafter, this group will be referred to as the users.

PROCEDURES/GUIDELINES

1. Conditions of Use

- 1.1 To protect the computing environment at the university, and ensure that the computing and network resources are available to all users, the computing and resources network will be used only for UFV-related work. In order that this work may be done in an atmosphere of trust and respect, UFV will provide these resources with the fewest possible restriction.
- 1.2 The computing and network resources must be used in accord with the public trust through which they have been provided, and in accordance with the rules and regulations established from time to time by the university. Users are accountable for their use of these resources, and for ensuring that they are being used as intended. Users located off campus are responsible for their use of the resources as though they were on campus.
- 1.3 The computing and network resources at UFV are provided to teaching, administrative, and service units, and in some particular circumstances, to the public. In some cases, users are provided with computer accounts on a UFV resource, and in others with access to computer stations. Resources may be provided to individuals, or to groups. Under any of these circumstances, UFV policies apply, and the responsibilities of users remain the same.
- 1.4 Users are prohibited from using the computing and network resources for purposes unrelated to the goals of UFV, or in ways which violate UFV policies or the laws of Canada.

Violation of UFV policies or laws of Canada includes, but is not limited to the following:

- Entry into UFV computing and network resources by individuals not specifically authorized (shall be viewed as trespass).
 - Attempts to circumvent the protective mechanisms of the University system (shall be considered attempted theft or trespass).
 - Deliberate attempts to degrade system performance or capability, or attempts to damage the systems, software or the intellectual property of others (shall be viewed as criminal activity).
 - Irresponsible use that which negatively affects the work of others (shall be viewed as an abuse of user privileges or mischief).
- 1.5 The university reserves the right to withhold access to computing and network resources if there are reasonable grounds to believe that continued access to the resources would pose a threat to the operation and availability of the resource or the good name of the university. Where there is substantiated abuse of computing privileges, UFV may remove a user's access to the resources (*section 6.1 for complete procedure). Both the threat posed to the community and the inconvenience to the user will be considered in this decision. The university will inform the user of available options to have computing and network privileges reinstated.

2. Privacy, Security and Integrity

- 2.1 UFV will treat the data and documents of users as private and confidential and will not examine information, or disclose it to a third party, without just cause or due process in the context of a disciplinary or criminal investigation.
- 2.3 All users must comply with the Copyright Act of Canada.
- 2.4 UFV will not normally monitor individual usage of any computing and network resources, although all general facilities may be monitored from time to time for the purposes of auditing and determining general usage patterns. This type of monitoring does not include the inspection of an individual's files or messages.
- 2.5 UFV will monitor and record usage where the violation of any UFV policy or illegal behaviour has been reported or detected. Such monitoring will only be done after consultation between the Director of Information Technology Services (or designate) and the appropriate Vice-President (* section 6.1 for complete procedure). UFV has the right to use the information obtained in disciplinary or criminal proceedings.

The nature and type of all monitoring incidents will be reported annually (May meeting) to the Senate by the Director of Information Technology Services.

- 2.6 UFV may copy (backups) or remove data files, user files, and system resources in the regular course of duties to preserve an efficient and accessible system.

3. Provisions for Research

- 3.1 Authorized use of UFV's computing and network resources includes the pursuit of legitimate research.
- 3.2 Users will be sensitive to the public nature of UFV's computing and network resources, and will not transmit or display on their workstations or screens any images, sounds or messages which might create an atmosphere of discomfort or harassment for others. If legitimate research requires the transmission of images, sounds or messages which others might find offensive, it is the user's responsibility to make special arrangements to minimize the possibility of offense to others.
- 3.3 Students should seek written authorization for special arrangements, including a description of the proposed research, from the instructor of the class for which the research is being done. This authorization should be taken to the Director of the UFV Library (or designate), who will help the student make the necessary privacy arrangements.
- 3.4 Faculty and staff should seek authorization for special arrangements from the Deans of instructional areas, or the supervisors of employees in other areas.
- 3.5 Special arrangements will not normally be made for members of the general public.
- 3.6 In the absence of such arrangements, the receipt, transmission or display of offensive images, sounds or messages will be considered a violation of this policy.

4. Investigation of Abuses of Computing Privileges

- 4.1 System administrators of computing and network resources have the responsibility to take remedial action in the case of possible abuse of computing and network privileges, and nothing in this policy diminishes that responsibility. The Director of Information Technology Services, or designate, after consultation with the appropriate Vice-President, and with due regard for the privacy of users, has the right to monitor use, suspend or modify privileges, examine files, passwords, accounting information, printouts, tapes, and any other material which may aid in the investigation of possible abuse. Whenever possible, the cooperation and consent of users will be sought in advance, and users given the opportunity to remove confidential files. However, for whatever reason, if system administrators are not able to obtain this permission, they may use extraordinary means to maintain the integrity of UFV computing and network resources. Users will be notified after the fact if such means have been used.
- 4.2 Investigation into suspected violation of this policy, as well as disciplinary action taken, will be governed by UFV policies and regulations, and applicable collective agreements. For example, where an academic offense such as plagiarism is involved, the same officers involved in a more traditional case will be involved in this one.
- 4.3 Supervisors of computing and network resources shall ensure that this policy and related explanatory materials, are posted and readily available to all users.

Reference: The Board policy on Development and Review of Administrative Policies (BRP-220.06) empowers the President to create and revise policies and procedures consistent with Policy Directions of the Board. This policy is guided by Board policy direction Risk Management (BPD-220).