Number 14
Effective Date 2021-12-13
Next Review Date 2026-12

APPROPRIATE USE OF INFORMATION TECHNOLOGY RESOURCES

Approval Authority	President
Responsible Executive	Chief Financial Officer and Vice-President Administration
Related Policies / Legislation	Board policy direction Risk Management (BPD-220) Prevention, Education and Response to Sexualized Violence policy (236) Copyright Compliance policy (7) British Columbia Freedom of Information and Protection of Privacy Act ("FIPPA")

PURPOSE

The purpose of this policy is to define the acceptable use of information management systems and technology under the control or custody of the University of the Fraser Valley (UFV), including protecting the personal privacy of its users and the security of its data management systems as required under the British Columbia Freedom of Information and Protection of Privacy Act ("FIPPA").

This policy establishes the responsibilities of the users of UFV technology regarding the appropriate use of university information and technology resources.

SCOPE

This policy applies to all users of information and technology resources (IT resources) as defined, below**.**

DEFINITIONS

In this policy, the following definitions apply:

Applicable laws: The laws of the province of British Columbia and the laws of Canada applicable to this policy.

Information and technology resources (IT resources): The information and technology resources the university makes available to users, including, but not limited to: Internet; Wi-Fi; email; networks; servers; computers; laptops; communications applications, licensed software (including third party software-as-a-service and cloud services tools); hardware; Intranet; mobilephones, tablets and other wireless communications devices; electronic storage media such as CDs, USB memory sticks, and portable hard drives; telephone and voicemail systems;

printers; plotters; scanners; cameras; fax machines; and all related equipment, peripherals and infrastructure (collectively, the "IT resources").

Sensitive information: personal information (as defined in FIPPA) pertaining to students, staff, or other individuals (i.e., student records, educational records, staff employment files, etc.) and/or confidential information of or about UFV, its business, operations, programs or plans that is not generally known, used or available to the public.

User(s): All UFV students, staff, faculty, and any other individuals who use the IT Resources, whether that access is during normal working, teaching, or class hours, and whether the resources are accessed at the University's campuses or remotely.

POLICY

The University of the Fraser Valley (UFV) seeks to provide a working and learning environment in which all persons are treated with dignity and respect, including in relation to the use of university information management systems and technology.

The University is also committed to ensuring the personal privacy of its users and the security of its data management systems as required under the British Columbia *Freedom of Information and Protection of Privacy Act* ("*FIPPA*").

This policy should be interpreted in a manner that is consistent with UFV's legal obligations, including its obligations under any applicable collective agreements, the terms of employment applicable to non-unionized staff, software license agreements or the university's obligations under *FIPPA*.

REGULATIONS

1. All users are responsible for their use of the IT resources and using them in compliance with this policyand other applicable laws.
2. All users are expected to notify the University if they become aware that IT resources are not being used in compliance with this policy.
3. All users must ensure that their use of the IT resources complies with all applicable laws, legal requirements, and ethical standards, including *FIPPA*, Canada's *Anti-Spam Legislation* ("***CASL***"), the Canadian *Criminal Code*, the Canadian *Copyright Act*, the BC *Civil Rights Protection Act,* and the British Columbia *Human Rights Code*
    - all University policies, including those concerning ethical conduct, standards of student andemployee conduct, and bullying and harassment;
    - third party software license agreements and third-party intellectual property rights;
    - the requirements of this policy; and
    - all employment agreements or collective agreements applicable to the user's use of the IT resources.

Prohibited activities - General

4. All users are expected to conduct themselves reasonably in the use of IT resources and to exercise good judgment. Specifically, except as permitted by this policy, IT resources cannot be used for transmitting, retrieving, creating, downloading, or storing any communication, file or information that is:
    - discriminatory, harassing, threatening, or advocating violence;
    - promoting hatred or contempt of any group or class of persons;
    - obscene, sexually explicit, or pornographic;
    - defamatory, libelous, abusive, or threatening;
    - encouraging of conduct or engaging in conduct that would constitute a criminal offense or giverise to liability to the University;
    - contrary to UFV's *Prevention, Education and Response to Sexualized Violence* policy (236);
    - misrepresenting or misleading with regard to the sender's identity;
    - an infringement of copyright, trademark, trade secret or other intellectual property rights;
    - in furtherance of an unauthorized access of other accounts, files, programs, communications, or information;
    - in violation of any license governing the use of software or third-party intellectual property rights;
    - collection, use, or disclosure of any personal information contrary to UFV policy and/or the Freedom of Information and Protection of Privacy Act (FIPPA Act).

Prohibited activities – Infrastructure

5. Any uses of the IT resources that disrupts or interferes with the operation of these resources or the ability of other users to utilize them for their intended or authorized purpose are prohibited. Such prohibited activities include but are not limited to:
    - destroying, altering, overriding, overloading, dismantling, disfiguring, or disabling IT resources;
    - damaging or altering the hardware or physical components of IT resources;
    - attempting to circumvent security controls on IT resources;
    - downloading, altering, plagiarizing, improperly appropriating or storing data or programs in breach ofsoftware license, copyright laws or third-party intellectual property rights;
    - knowingly introducing malware including viruses, worms, Trojan horses, and spyware to IT resources;
    - intercepting or examining the contents of messages, files, communications, accounts, or programs without appropriate authorization; and
    - engaging in any uses that results in the unauthorized examination, interception, dissemination,destruction, loss, theft, or alteration of another user's information.

6. Notwithstanding the foregoing, nothing in Clause 4 or 5 above shall be construed as preventing or restricting duly authorized: (a) system administrators or other technical personnel from carrying out their regular job duties; or (b) faculty, instructors, or students, in the course of teaching or carrying research or other academic activities, provided that such activities falling within the scope of Clause 5 are first approved in writing by the Chief Information Officer (CIO).

Security

7. Users must take appropriate steps to ensure the security of the IT resources by adhering to all applicablesecurity measures, including using and safeguarding all necessary passwords.

8. Users are expected to choose secure complex passwords and avoid using passwords that use sequencesor common words (such as “12345”, “ABCDE”, “55555”, etc.) or public knowledge items that relate to users personally (such as a user’s name, address, phone number or spouse’s name). Passwords used tosecure IT resources shall not be used by the user for other purposes or on personally held online accounts with third parties.

9. Sharing passwords or using another user’s password constitutes a violation of system security and is prohibited.

10. All users must ensure that their IT resources are secured when they are not being used, including logging out of devices at the end of the workday or class.

Working away from the office

11. Faculty and staff must have authorization from their department head or supervisor before accessing sensitive information from remote work locations.

12. To the extent practicable, access to and use of sensitive information when working remotely should takeplace via secure virtual private network, rather than storing such information locally on mobile devices or personal devices.

13. Faculty and staff should avoid accessing or viewing sensitive information except via secure wirelessnetworks. Public networks are not secure.

14. Faculty and staff who use home computers or personally owned devices (“personal devices”) to store oraccess sensitive information must ensure that access to the sensitive information is not provided to any other users of such personal devices.

15. Faculty or staff members who store sensitive information on personal devices may be requested to produce personal devices for inspection of any files containing sensitive information to ensure compliance with this policy. Faculty and staff are expected to comply with any direction to securely destroy sensitive information if stored on personal devices.

16. Faculty and staff must ensure that sensitive information stored on mobile devices (smart phones, flash drives, laptops, tablets, external hard drives) ("mobile devices") is secure against risks such as loss, theft, or unauthorized access, including by keeping mobile devices physically secured and by ensuring that devices are password protected and files containing sensitive information are securely encrypted.

17. Sensitive information when stored on mobile devices or personal devices must be encrypted andsecurely destroyed when no longer needed.

18. Faculty and staff must not use personal email accounts for university business, including, but not limitedto the storage, transmission, or disclosure of sensitive information.

19. UFV is subject to *FIPPA* legislation, which permits members of the public to request records within its custody and control. Employees who store university files or data on personal devices (including via text message, video footage, personal email accounts) may be required to provide copies of such records to the university.

Cross-border travelling with IT resources

20. If users need to travel outside of Canada with IT resources or any sensitive information, users should only bring the sensitive information they reasonably require having while travelling.

21. Outside of Canada, sensitive information must only be accessed using a secure virtual private network.
    Sensitive Information should not be stored or carried either physically in the form of paper orelectronically via devices such as a phone, laptop, external hard-drive, or USB memory stick.

Personal Use

22. Unless otherwise permitted in this policy, IT resources are to be used only for purposes that are directlyrelated to university business.

23. Notwithstanding Clause 23, incidental personal use of the IT resources is permissible provided that suchuse does not interfere with the user's performance of their employment or other duties to the university. Incidental personal use of the IT resources must meet all the following criteria:
    - it is infrequent and of short duration, or it occurs outside of working or instructional hours;
    - it complies with this policy and applicable laws;
    - it does not cause the university to incur any cost;
    - it does not expose the university to any harm, risk, loss, or liability;
    - it does not involve downloading or viewing material that promotes racism, sexism, violence,hatred or contempt of any group or class of persons or is pornographic; and
    - it is not part of any activity which the user engages in for commercial purposes or personalprofit.

24. While UFV does not encourage personal use of its IT resources, the University recognizes that where such use takes place, its IT resources may contain or store information or records relating to this personal use, e.g., personal emails, documents, voicemails, text messages, and records of internet and social media use ("personal use records").

25. While UFV takes reasonable measures to back up information and protect it from loss and unauthorized access, the University cannot guarantee that personal user records will be retained within the IT resources or remain confidential. Users who utilize the IT resources to create, store or circulate personal-user records do so at their own risk. The University will not intentionally access, use, or disclose personal user records, except as described in this policy, with user consent or as otherwise authorized do so under *FIPPA* or required by law.

26. UFV has a responsibility to ensure that all email, communications, data, and information downloaded, viewed, accessed, created, or altered using the IT resources complies with the University's policies, agreements, and applicable laws.

27. UFV does not engage in ongoing or routine monitoring of users' use of IT resources. However, regular monitoring may occur for legitimate reasons, including for trouble shooting, monitoring, and addressing network security and performance, addressing system maintenance needs, and evaluating and improving the University's systems.

28. The IT resources, and all use of or information contained or stored by the IT resources, may also be monitored, or accessed from time to time in order to:
    - manage employee transitions following the termination or departure of an employee on a longterm leave on approval of the CIO;
    - investigate incidents, complaints or allegations if there are reasonable grounds to believestudent or employee misconduct has occurred or is occurring, including any violation of UFV policies or agreements or applicable laws;
    - ensure that IT resources are being used in compliance with this policy, other University policies, and the law, including *FIPPA*; and
    - for other purposes where the University is authorized or required by *FIPPA* or other applicable laws to access or monitor.

29. Accordingly, the University does not guarantee privacy in the use of any IT resources, even where they used for incidental personal use. Users should be aware that the University has access to and may inspect anyinformation or materials stored, transmitted, or created using IT resources.

Discipline

30. Users who misuse the IT resources, or who otherwise breach this policy, will be subject to:
    - disciplinary action, up to and including termination of employment for cause or termination ofenrollment in a course of studies, as applicable; and/or
    - revocation or suspension of the user's access to or privileges to use IT resources.

Administration of this Policy

31 The University's CIO or their designate is responsible for authorizing the use of IT resources, providing appropriate training to users regarding awareness, providing guidance on compliance with this policy, and monitoring and investigating the use of IT resources reasonably, as necessary, or as requested and in accordance with *FIPPA*.

32. Any user who believes that IT resources are being misused, or that this policy is being breached, shouldreport the alleged violation immediately to UFV's CIO or designate, who will be responsible forinvestigating reported or suspected violations of this policy.

33. All monitoring, searching, or accessing IT resources by the University under section 28, must be approved by UFV's CIO or designate.