S.08-132

Senate for Information
Board Committee to Recommend
Board to Approve

SIMON FRASER UNIVERSITY

POLICY REVISION: GP 24 FAIR USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT)

4 November, 2008

1. To Senate for information

2. To the Board of Governors for approval:

Motion

"That the revision of Policy GP 24 Fair Use of Information and Communications Technology (ICT) be approved to take effect immediately"

Background (see attached)

Submitted by:

W. Krane
Associate Vice-President, Academic
and Associate Provost

P. Hibbitts
Vice-President Finance
and Administration

I concur and recommend to the Board:

Jon Driver, Acting President

SFU SIMON FRASER UNIVERSITY
CIO | CHIEF INFORMATION OFFICER

MEMORANDUM

TO: Bill Krane
Cc K.C. Bell

FROM: Jim Cranston

RE: GP-24 - Fair Use of ICT - Revisions

DATE: Nov 3, 2008

In March 2008, a revised GP-24 – Fair Use of ICT – was submitted to the SFU community for their review and input. We received comments (5) on this draft and have made revisions to accommodate the expressed concerns as follows:

1 Much more explicit reference to the FOIPOP law and changes to wording that contradicted it. Ian Forsyth has provided direction in this regard and I think we now conform to legality.

2 Added sections to deal with Disclosure of Information for purposes of Administrative Continuity (2.2.3) and Role Accounts (2.2.4). These provide a less onerous mechanism to access information strictly for administrative purposes in cases where an employee is absent. If information is released under this provision it must not be used for any other purpose, such as an investigation.

3. Removed all the references to "file attributes denoting privacy" etc. as this seemed overly complicated and probably meaningless. Basically this implies that if information is stored on SFU's ICT equipment we have the right to access it according to our protocols.

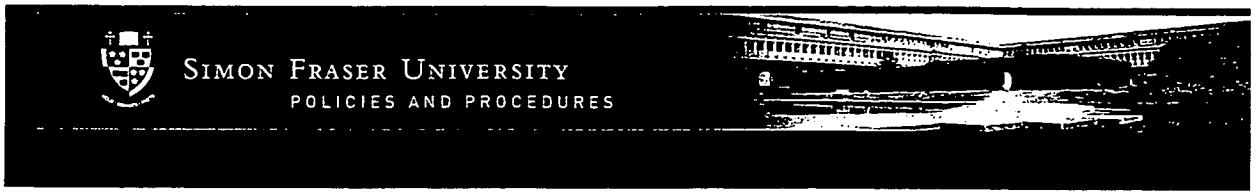
4. We made a few changes/additions to definitions and minor clarification suggested by some people.

I recommend that this version be taken forward to the SCUP/Senate for information and subsequently to the Board for approval and implementation

Please advise if you have any questions.

2.

Jim Cranston, CIO Tel: 604-291-5807 e-Mail: jim_cranston@sfu.ca



SIMON FRASER UNIVERSITY	Date	Number
Policies and Procedures	March 1993	GP 24
	Revision Date	**Revision No.**
	November 3, 2008	1.1 (Draft 1.12)

Subject: Fair Use of Information and Communications Technology (ICT)

Preamble

This policy allows those who administer the University's Information and Communications Technology (ICT) resources to do so as transparently as possible, while providing users with essential guidance on their rights and responsibilities.

ICT resources (see section 6) include business tools that facilitate University processes and activities related to its research, teaching and community service mandates. The University recognizes those resources may be the pathway by which controversial points of view and new ideas are disseminated and tested by members of the community.

The University continuously strives to create an environment that provides members of the community with the resources needed to meet the objectives of their work and/or studies, and to create a working and learning environment that promotes full, free and responsible participation by all members.

1.0 Purpose:

1.1 The Purpose of this policy is to:

a) establish the University's right to control and manage its Information and Communications Technology (ICT) resources;

b) inform administrators and users of SFU's ICT resources of their rights and responsibilities regarding the management and use of these fundamental resources; and

c) make users accountable for their use of the University's ICT resources.

2.0 Policy:

2.1 Right of Access

2.1.1 Authorized users of the University's ICT resources have the right to access them without interference by others.

2.1.2 Where users misuse the University's ICT resources, their right of access may be restricted or removed. . (See section 2.6.)

2.2 Confidentiality and Privacy Protection

2.2.1 General

The University respects the privacy of those who use the University's ICT resources and protects users' information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal. The University's ICT staff will comply with the FOIPOP Act and the University's information and privacy policies (I10.xx series) and will disclose a user's activities and personal information only as permitted or required by law.

2.2.2 Logging of Information

Most activities performed using the University's ICT resources are logged. Information in log files is owned by the University and is routinely examined by ICT support staff to monitor the performance, reliability and security of ICT resources. ICT support must not disclose information learned from or contained within these log files except when authorized in writing to do so by their Director in order to:

a) investigate an alleged violation of this Policy or other related University Policy using the procedure outlined in Appendix II; or to

b) respond to a request for information pursuant to proceedings under the auspices of another University Policy using the procedure outlined in Appendix II; or to

c) ensure administrative continuity (see sections 2.2.3 and 2.2.4).

2.2.3 Disclosure of Information - Administrative Continuity

In cases of the absence, retirement or termination of a employee engaged in administrative duties, there may be occasions where departments need access to that individual's emails or files to conduct business as permitted under section 33.2(c) FOIPOP Act. In such cases the Chair or unit head can obtain access by making a request to the Director, Client and Research Services (CaRS). Any information released under this provision may not be used for any employee discipline or other purpose except administrative continuity and any personal information shall be kept confidential.

2.2.4 Role Accounts

Role accounts (i.e., those granted to a role or organizational position rather than to an individual for business purposes) may be shared amongst authorized users as determined by the appropriate Department Chair/unit head. Information contained in these accounts may be accessed and disseminated upon the request of the Chair/unit head to the Director, Client and Research Services (CaRS). Users are advised that role accounts should not be used to store personal information as they are subject to access should the University need to do so to conduct its operations.

2.3 Personal Use

2.3.1 Accounts to access ICT resources are issued for the sole use of the person to whom they are issued. Accounts are not to be shared, given, rented, sold or reassigned to any other individual or organization. Role accounts are exceptions to this provision

2.3.2 Incidental personal use of ICT resources is allowed provided that it does not: contravene the law and provisions of this or other University policies; interfere with access to ICT resources by authorized users; or cause the University to incur additional costs (e.g., excessive use of internet bandwidth).

2.4 Commercial Use

2.4.1 The University's ICT resources shall not be used for commercial purposes, for profit-making, or for the benefit of non-SFU organizations unless these purposes are authorized under, and consistent with, the appropriate University policies and procedures. This provision shall not restrict SFU researchers from pursuing their research activities and freely exchanging information.

2.5 Misuse

2.5.1 Misuse of the University's ICT Resources is explicitly prohibited. Activities included under the definition of "misuse" are set out in *Section 6.0 Definitions* below.

2.6 Protective Measures

2.6.1 The University reserves the right to limit, restrict or terminate user access and to inspect, copy, remove or otherwise alter any data, files or other ICT resources covered by this policy.

2.6.2 At the direction of the Director, CaRS or designate, interim measures may be taken by duly authorized ICT staff in immediate response to allegations or awareness of misuse. These measures shall remain in force until the matter is resolved by the appropriate University Officer.

3.0 Scope:

3.1 This Policy applies to anyone using the University's ICT resources or using their SFU authorization credentials to access ICT resources provided by other organizations. In the latter case, users are responsible for making themselves aware of, and to comply with, the other organization's "acceptable use" policies.

3.2 This Policy covers all University-owned or -leased ICT resources, whether individually controlled or shared, standalone or networked, and to all activities of individuals accessing University-owned ICT resources from non-University-owned ICT resources. (e.g., personal computer, PDA, or other devices).

3.3 From time to time the University may grant access to ICT resources to persons from other organizations through reciprocal sharing agreements with individual organizations or through participation in a federation of organizations. This privilege may be revoked solely at the discretion of the University.

4.0 Roles and Responsibilities:

4.1 The University's ICT resources will be provided and protected by the University to a degree that is reasonable and technically feasible under the guidelines set out by this policy, its associated procedures, section 30 of the FOIPOP Act and any other relevant University policy or procedure (see Appendix 1 for a partial list of such documents).

4.2 The University warrants that it makes reasonable security arrangements for the ICT resources offered; however, SFU stipulates that there are no guarantees regarding the accessibility, reliability or security of said resources.

4.3 The responsibilities of the ICT staff, in priority order, are to maintain the security of the information in the ICT environment, maintain the ICT environment in an operationally available state, and ensure that the ICT resources are accessible to the members of the user community. Where the security of information within the ICT environment is threatened, access to the environment may be restricted until the threat is resolved.

5.0 Authority:

5.1 This policy is administered under the authority of the Chief Information Officer.

6.0 Definitions

Authorization for File Access is the Form required to view information either owned by an Authorized User or pertaining to an Authorized User for which the User has not given permission, except for role accounts (section 2.2.4) or in situations dealing with Administrative continuity (section 2.2.3). An Authorization is normally required to support an investigation or process associated with the application of this or another University Policy.

Authorized Users are those who have current ICT identity credentials granted by an authorized 0fficer of the University.

Confidentiality means keeping personal information private or secret, safe from access, use or disclosure by people who are not authorized to handle that information. (BC Govt. FOIPOP Policy and Procedures Manual).

FOIPOP Act refers to the *Freedom of Information and Protection of Privacy Act* and associated Regulations enacted by the Province of British Columbia. Also known as FOIPOP.

ICT Resources Information resources in this document are meant to include any information in digital format, or any hardware or software that make possible the electronic storage and use of such information. This includes, but is not limited to, electronic mail, local databases, externally accessed databases, CD-ROM, motion picture film, recorded magnetic media, photographs, and digitized information. For purposes of this Policy, the "appropriate use of ICT resources" does not refer to managing digital information in terms of its classification, organization, retention or disposal; this is not a records management policy.

Interim measures may include, but are not limited to:

- contact with respondents to establish the veracity of allegations;
- discussions with respondents to informally resolve problems;

- instruction to respondents to cease and desist alleged misuse within a time limit; or
- temporary disabling of respondents' computer accounts or other access.

It is understood that interim measures are to be preemptive and remedial rather than punitive and will remain in force until the matter is resolved by the appropriate University Officer.

Misuse under this policy encompasses, but is not limited to:

Unlawful Activities:

- Any activity that contravenes federal or provincial legislation, whether or not the activity is reported to the police
- The evidence supporting a suspicion or allegation of unlawful activity will be assessed and misuse will be determined based on a 'Balance of Probabilities' standard
- Knowledge of and compliance with the law is the responsibility of the user

Threats to System Security or Integrity:

- Seeking to gain, or gaining, unauthorized access to ICT resources
- Possessing, creating, transmitting or storing tools, programs, attachments or other materials for the purpose of gaining unauthorized access
- Examining or using without authorization another user's files or programs in transit or in storage
- Unauthorized scanning of other computers on the network
- Preventing rightful access to computer-based information and ICT resources
- Altering, disrupting or otherwise interfering with the integrity of computer-based information and ICT resources, including the passing on of viruses, worms, "trojans" or other "malware"
- Endangering the finite capacity of any system through "chain mail," "flame wars," "bombing," "spamming" or using any method system administrators consider may endanger and/or restrict the access to their accounts by other authorized users
- Impersonating another user (regardless of whether the other user is real or fictitious) by altering individual system identity

Excessive Use of ICT Resources:

- Use of ICT resources in a manner that may result in additional cost to the University
- Use of ICT resources in a manner that consumes resources that would rightfully be available to others.

Contravention of University Policy

- Use of ICT Resources contrary to another University policy will be addressed as applicable under the relevant policy.

Personal is defined as relating to, concerning, or affecting a person as a private individual (rather than as a member of a group or the public, or in a public or professional capacity); individual, private; one's own.

Personal Information means recorded information about an identifiable individual other than contact information (FOIPOP Act).

Privacy means the state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; seclusion, freedom from interference or intrusion. (BC Govt. FOIPOP Policy and Procedures Manual)

Record 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 (FOIPOP Act). Note that this definition of "record" specifically excludes ICT resources (i.e., a computer program or any other mechanism that produces records).

Appendix I

This Policy should be read and understood in conjunction with the following University Policies and documents, and with the University's Statement on Values and Commitments:

- A 30.03 Faculty Code of Ethics
- AD 1.06 Commercial Activities and Advertising
- AD 1.12 Selling, Serving and Advertising Liquor
- GP 18 Human Rights
- GP 25 Response to Violence and Threatening Behaviour
- GP 30 Interpretation Policy
- I 10.04 Access to Information and Protection of Privacy
- R 30.01 Copyright Policy
- T 10.01 Code of Student Conduct
- T 10.02 Code of Academic Honesty
- Applicable Residence and Housing agreements/contracts

Appendix II – Procedure to Authorize File Access

An Authorization for File Access is required to view information either owned by an Authorized User or pertaining to an Authorized User for which the User has not given permission, except for role accounts (section 2.2.4) or in situations dealing with Administrative continuity (section 2.2.3). An Authorization is normally required to support an investigation or process associated with the application of this or another University Policy.

Log files and file directories are system resources and are routinely monitored by duly authorized system support staff to maintain the security, reliability, accessibility, and performance of the University's ICT resources. Notwithstanding these, systems staff must not divulge any information pertaining to the activities of an Authorized User to anyone other than other duly authorized system support staff.

Neither the Authorization forms nor the information arising from their use may be transmitted via any insecure communications media. E.g., email is neither acceptable nor sufficient.

1. If the Authorization for File Access is sought to support an allegation or suspicion of misuse under this policy, an Authorization for File Access Form must be completed by the person making the claim.

2. If the Authorization for File Access is sought to support the application of another University Policy, the Authorization for File Access Form shall be completed by the person duly appointed to investigate under the auspices of the applicable University Policy.

3. The Authorization for File Access must contain the following information:

   - The name of the applicant
   - The date of the application to access the files
   - The ID of the Authorized User for which the application is requested
   - The date that the file access must cease/end
   - The Name of the Authorized User for which the application is requested
   - The University Policy under which the application is requested
   - A description containing the reason for the request and the information requested
   - The names of staff/faculty who are authorized to access this information when it is produced
   - The name, phone number, and signature of the person requesting the information

4. The completed Authorization for File Access form should be taken to the Director, CaRS. The request will be reviewed to ensure that the information requested is possible to produce, that it is sufficient to meet the objective of the request, and that the resources required to produce the information are available. (Note: Requests for information from backup tapes or log files can take several days to produce.) If the Director, CaRS agrees with the technical aspects of the requests and has the resources available to produce the information the Director, CaRS will approve the form.

5. The Director, CaRS will then take the form to seek the approval of two University Vice-Presidents. The requestor may or may not accompany the Director when seeking the Vice-Presidents' approval.

6. The information will be assembled and two copies prepared on an appropriate storage media (usually a write once CD or DVD). The information will be assembled by the appropriate systems support person, who will initial the media in order to identify it later if necessary. One copy will be stored in a confidential file with the original of the approved Authorization for File Access form, and the second will be given to the requestor.

Appendix III – Authorization for File Access

Sample Form Attached

SFU **Simon Fraser University IT Services**

REQUEST FOR ACCESS TO INFORMATION CONTAINED IN ICT RESOURCES

This is a request for members of the Computer Security Team of IT Services to access and monitor the computer data files of the following computing account. This monitoring will commence immediately and may remain until 24:00 hours of the End Date.

Computing ID: _____ Owners Name: _____

End Date: _____

Reason for Request:

This request is to provide information to support University Policy _____
The specific reasons supporting this request are as follows: _____
_____
_____

Authorized Personnel:

The information contained in the files of the above listed account will only be made available to authorized personnel. Authorized personnel include the members of the Computer Security Team of IT Services, the University Vice-Presidents, the person leading the investigation and others so designated on this form. Furthermore, these authorized people will not be granted access to the information until they have agreed not to disclose or discuss the information with people not authorized on this form.

Other Authorized Persons: _____

_____

The Requestor:

Name _____ Signature _____Phone: _____

Approvals:

This request requires the approval of a Director in the IT Services group performing the examination and the approval of any two University Vice-Presidents.

Director CaRS: _____

Vice-President _____

Vice President _____

Return to web view

SIMON FRASER UNIVERSITY

Policies and Procedures

Date	Number
March 23, 1993	GP 24
Revision Date	**Revision No.**

POLICY AND PROCEDURE ON THE FAIR USE OF INFORMATION RESOURCES

1. **University Information Resources**

Simon Fraser University makes computing and other information resource facilities available to its faculty, staff, students, and authorized external users. The goal of the facilities offered to these users is to provide an open and effective information technology infrastructure for instructional, research, and administrative use. Users have the right to expect that their rightful access to information, their use of network and equipment authorized to them, and their use of any other resources connected with their authorized access to services will be protected by the University to a degree that is reasonable and technically feasible. In order to preserve the integrity of the facilities against accidents, failures or improper use, the University reserves the right to limit, restrict or terminate any user's access, and to inspect, copy, remove, or otherwise alter any data, file, or system resources within the limitations set out below.

The use of the University's information resources is extended to members of the University community to help them meet the objectives of their studies, research, or job-related tasks.

The University makes no warranty, express or implied, regarding the computing services offered, or their fitness for any particular purpose. The computing facilities provided will be designed to serve the broad base of users in the community, but cannot be expected to fulfill every specialized need.

2. **The Proper Use of Information Resources, Information Technology, and Networks**

It is the policy of the University to maintain access for its community to local, national and international sources of information and to provide an atmosphere that encourages access to knowledge and sharing of information.

It is the policy of the University that information resources will be used by members of its community with respect for the public trust through which they have been provided and in accordance with policy and regulations established from time to time by the University and its operating units.

In accordance with the above policies, the University works to create an intellectual environment in which students, staff, and faculty may feel free to create and to collaborate with colleagues both at the University and at other institutions, without fear that the products of their intellectual efforts will be violated by misrepresentation, tampering, destruction and/or theft.

Access to the information resource infrastructure both within the University and beyond the campus, sharing of information, and security of the intellectual products of the community, all require that each and every user accept responsibility to protect the rights of the community. Any member of the University community who, without authorization, accesses, uses, destroys, alters, dismantles or disfigures the University information technologies, properties or facilities, including those owned by third parties, thereby threatens the atmosphere of increased access and sharing of information, threatens the security within which members of the community may create intellectual products and maintain records, and in light of the University's policy in this area, has engaged in unethical and unacceptable conduct. Access to the networks and to the information technology environment at the University is a privilege and must be treated as such by all users of these systems.

To ensure the existence of this information resource environment, members of the University community will take actions, in concert with government agencies and other interested parties, to identify and to set up technical and procedural mechanisms to make the information technology environment at the University and its internal and external networks resistant to disruption.

In the final analysis, the health and well-being of this resource is the responsibility of its users who must all guard against abuses which disrupt and/or threaten the long-term viability of the systems at the University and those beyond the University. The University requires that members of its community act in accordance with these responsibilities, this policy, the University's Harassment Policy, relevant laws and contractual obligations, and the highest standard of ethics.

Though not exhaustive, the following defines the University's position regarding several general issues in this area.

a. Information resources in this document are meant to include any information in electronic or audio-visual format or any hardware or software that make possible the storage and use of such information. As example, included in this definition are electronic mail, local databases, externally accessed databases, CD-ROM, motion picture film, recorded magnetic media, photographs, and digitized information.

b. The University characterizes as unethical and unacceptable, and just cause for taking disciplinary action up to and including non-reappointment, discharge, suspension, expulsion, dismissal, financial penalties and/or legal action, any activity through which an individual:

   i. violates such matters as University or third party copyright or patent protection and authorizations, as well as license agreements and other contracts;

   ii. interferes with the intended use of the information resources;

   iii. seeks to gain or gains unauthorized access to information resources;

   iv. without authorization, destroys, alters, dismantles, disfigures, prevents rightful access to or otherwise interferes with the integrity of computer- based information and/or information resources;

   v. without authorization invades the privacy of individuals or entities that are creators, authors, users, or subjects of information resources;

   vi. makes pre-emptive use of the system for personal gain.

c. This policy is applicable to any member of the University community, whether at the University or elsewhere, and refers to all information resources whether individually controlled, or shared, stand-alone or networked. Individual units within the University may define conditions of use for facilities under their control. These statements must be consistent with this overall policy but may provide additional detail, guidelines and/or restrictions. Where such conditions of use exist, enforcement mechanisms defined therein shall apply. Where no enforcement mechanism exits, the applicable general policies and agreements of the University shall prevail. Where use of external networks is involved, policies governing such use also are applicable and must be adhered to.

3. **Rights and Obligations of University Staff**

The staff of University service units in general have the right, within their jurisdiction, to carry out their responsibility to keep the University's information technology facilities operating and available to the user community.

It is acknowledged that there is a delicate balance between the absolute right of privacy of a user, and the need of the staff to investigate and correct disruptions in order to insure the continued functioning of the facilities.

In exceptional circumstances, where it is deemed necessary to protect the integrity of the system, designated staff members authorized by two designated senior administrators of the University may be permitted to examine stored or printed data to gather sufficient information to diagnose and correct problems, or to determine if a user is acting in violation of University policy. In doing so, the staff has an obligation to maintain the privacy of a user's data.

4. **Procedure**

A copy of this policy shall be made available to all computing account holders.

A banner notice comprised of a brief summary of this policy shall be displayed when a user signs on to the system.

The University Computing Advisory Committee shall establish a Computer Security Task Force to investigate allegations of misuse of the University's computing and other information resources. All members of the University community are encouraged to cooperate with such inquiries.

Upon completion of the investigation, the Chair of the Task Force shall determine whether prima facie evidence of misuse exists. A negative determination will result in no further action and no record of the allegation. If a positive determination is made, a detailed and complete report of the results of the investigation will be forwarded to a disciplinary body for action. The disciplinary body appropriate to the case will depend on the status of the alleged misuser of the resources.

Return to web view