POLICY ON COMPUTING FACILITIES

Effective Date: March 8, 1999

Originating Office: Office of the Vice-President, Services

Supersedes /Amends: VRS-30/October 1, 1997

Policy Number: VPS-30

SCOPE

This policy applies to all members of the University and to all authorized users of the Concordia Computing Facilities.

DEFINITION

For the purposes of this policy:

> *Concordia Computing Facilities ("CCF")* are defined as any computer, computer based network, computer peripheral, operating system, software or any combination thereof, owned by the University or under the custody or control of the University. Equipment and software purchased from research funds administered by the University are owned by the University unless otherwise specified in the research grant or contract.

PREAMBLE

The CCF are made available to students, faculty members, staff, alumni and others for the purpose of advancing the academic goals of learning, teaching and research and for assisting in administrative operations which support these goals. It is the responsibility of all users to ensure that they are not wasting the resources, interfering with the work of others or breaching applicable policies and legislation.

POLICY

General

1. While Instructional and Information Technology Services (IITS) acts as a central provider of computing and other information technology resources, the overall information technology infrastructure is a distributed and shared environment. The distributed management is performed by individuals generally known as Systems Administrators. Collectively, they are referred to as the Concordia Computer Systems Administrators (CCSA). IITS will convene regular meetings of the CCSA for information and coordination purposes.

2. In order to preserve the integrity of the CCF against accidents, failures or improper use, the University reserves the right to limit, restrict or terminate the access of any user to these facilities or the access of any host or equipment to the network, and to inspect, copy, remove or otherwise alter any data, file, or system resources. The CCSA will act on behalf of the University in such eventuality.

3. The University makes no warranty, expressed or implied, regarding the resources and facilities offered or their fitness for any particular purpose. The CCF are designed to serve the broad base of users in the community but cannot be expected to fulfill every specialized need.

Appropriate Use

4. Access to the CCF is intended for the pursuit of the academic mission and administrative functions of the University and shall not be used for commercial gain or unsolicited advertising except by University departments and subcontractors acting within the parameters of their University-defined missions. Indirect (such as web-based) advertising is similarly permitted only within those parameters. As such, it is forbidden to sell advertising space on University web pages unless otherwise permitted by University policy.

5. Access to the CCF shall not be used for unsolicited mass mailings of any kind including chain letters and advertising except by University departments and subcontractors acting within the parameters of their University-defined missions. Unsolicited mass e-mailings should be used sparingly and may be made only through distribution channels approved by IITS.

6. A computer username and password is intended for the exclusive use of the person to whom it is issued. Sharing of usernames and passwords amongst authorized persons (i.e. the use of group accounts) is strongly discouraged. Sharing of usernames and passwords under any other circumstances is forbidden. All responsibility for the use of an account shall be borne by the person to whom a username is initially issued.

7. The University must ensure that it can trace any use of the network from within its organization to the individual who initiated that use. Therefore, the provenance of any e-mail or netnews message (or any other electronic communication) must be clearly

identified and accurate. For example, the "From" header of any such message must contain a valid address for a computer account under the control of the sender.

8. Use of any part of the CCF without the consent of the appropriate systems administrator is prohibited.

9. Users shall not attempt unauthorized access to computing resources either inside or outside of the University.

10. External networks and systems normally have their own set of rules and guidelines for usage. Users are expected to abide by these external rules and guidelines when accessing such a service.

11. Users shall not use the CCF to obtain and/or exchange proprietary software, information or other computer based material when such action violates the copyright of others.

12. Users shall not use the CCF for any unauthorized or illegal purpose, such as, but not limited to, the destruction or altering of data owned by others, the interference with legitimate access to computing facilities, the disruption of the CCF, the attempt to discover or alter passwords or to subvert security systems in the CCF or in any other computing facility.

13. Users shall not use the CCF to send obscene, vulgar or harassing messages by electronic mail or by other means. University policies and legislation exist to address such abuse and shall be invoked.

Computer Access

14. Particular members of the University are granted the privilege of free, limited access to certain components of the CCF via the public systems made available by IITS. The following list defines most of the eligible groups:

    a. Full-time and part-time students at all levels of study;

    b. Full-time and part time faculty members, Adjunct Professors and Post-Doctoral Fellows;

c. Full-time administrative and support staff and part-time administrative and support staff in contract positions;

d. Individuals provided for by conditions in a collective agreement.

15. In addition to the groups listed in section 14, special arrangements may be possible, at the discretion of the Director, IITS.

16. The following groups are not automatically granted access to the CCF:

a. Continuing Education students;

b. Casual employees;

c. Collaborators of University researchers

17. While the basic level of network accessibility is equivalent, the different groups receive different levels of service due to resource limitations. Users have the right to use public access equipment, run programs on the computers assigned, use network services and store files.

18. Student usernames on the public systems remain in existence as long as the student remains registered and the account itself remains active. After a certain period of inactivity, defined in the IITS Operational Procedures, student accounts are deleted.

19. Student usernames assigned to graduate students remain in existence as long as the student remains registered or his or her faculty supervisor continues to authorize their activities.

20. Faculty and administrative and support staff may keep their usernames while they remain in the employ of the University. Faculty and administrative and support staff shall be notified on an annual basis of the computer usernames for which they are responsible. They are expected to notify IITS, or the appropriate systems administrator, in the event that they no longer require access to the CCF.

21. In the event that a member of the CCSA has reason to believe that a user is abusing the privilege of computer access, as outlined in this policy, other University policies or International, Federal or Provincial legislation, that user's computer access may be temporarily suspended pending further investigation.

22. Processes exist for handling various types of computer abuse and are outlined in the IITS Operational Procedures. The penalty for abuse of CCF privileges may include the loss of these privileges.

23. Incidents of computer abuse may, as well, constitute grounds for action pursuant to the *Code of Rights and Responsibilities*, the *Code of Conduct (Academic)*, collective agreements, other University policies or Federal or Provincial legislation.

Information Privacy

24. All users have the right to a reasonable expectation of privacy from other computer users.

25. Information held on the CCF is private to its owner unless specific action is taken by the owner to make the information available to others.

26. Much of the privacy of computer information relies on the degree of protection users place on their individual usernames and passwords. It is the responsibility of individual users to be aware of computer security and privacy risks, such as Trojan horse programs, viruses and the like. As outlined in section 6 of this policy, it is the user's responsibility to keep his or her password private from others.

27. Any activities such as browsing computer screens, recovering other user's garbage, physical theft of printouts and the like are prohibited.

28. Any actual or suspected violation of information privacy must be reported to the service areas of IITS or to the appropriate member of the CCSA. Failure to do so may be construed as effective consent to the action.

29. Information privacy shall continue to be respected following the expiration of a computer username.

30. Users are expected to be aware that different computer systems make certain information public to other users. The contents of individual files are never made available by default but events such as last commands executed, login time and username are often available to other users.

31. While the contents of e-mail are covered by the principle of information privacy, as well, users must realize that in the course of delivery, e-mail often passes between computer systems and these systems may not be bound by this policy. As such, sensitive material should not be transmitted via e-mail without special precautions.

32. In order to preserve the integrity of the CCF against accidents, failures or improper use, the University reserves the right to inspect, copy, remove or otherwise alter any data, file, or system resources that are part of the CCF. In particular, designated representatives of IITS, or CCSA members designated by their departments, have the authority to remove any materials from University facilities which they manage, when those materials, in the opinion of the representative, violate University policies or relevant legislation or are inappropriate to the intended use of the facility. This may include the implementation of automated methods to detect and remove such materials such as configuring mailers to reject "spam" messages.

33. The University does not, however, undertake to systematically audit its facilities for such material, in particular where materials can reasonably be placed on University facilities by people outside the University. As such, the University does not accept responsibility for materials received via electronic mailing lists, netnews and the like. It must be understood that where automated measures have been put in place, valid transmissions may be mistakenly removed. The University accepts no liability for the results of such removals.

34. The University reserves the right to inspect, copy, remove or otherwise alter any data, file or system resources that are part of the CCF, in order to assist any outside investigation of computer crime which involves the CCF. Where necessary to the investigation, the University may also share such information with the appropriate authorities.

35. Users should further recognize that authorized personnel of the CCSA have the obligation to take reasonable and appropriate steps to ensure the integrity of the CCF and to ensure that this policy is observed.

World Wide Web Publishing

36. Web pages are deemed to be either "Authoritative," that is, representing a department, service or academic program of the University or "Casual," that is, being used as an informal or non-official information resource.

37. All Authoritative pages shall conform to the University Identification Standards Manual (administered by the Department of Marketing Communications) as well as to the *Policy on the Use of the Name Concordia University and Related Insignia* (SG-4).

38. All Authoritative pages shall contain an indication as to when they were last updated as well as the e-mail address of the publisher of the page.

39. Publishers of Authoritative pages shall ensure that the pages are reviewed and updated appropriately.

40. If required, appropriate permission must be obtained by the publisher of any page held on the CCF prior to posting text, graphics, sounds or movies which are not of his or her own creation.

41. The University reserves the right to remove any pages from its CCF.