ACCEPTABLE USE OF COMPUTERS AND INFORMATION TECHNOLOGY

Part 1. Purpose

Subpart A. Acceptable use

This procedure establishes responsibilities for acceptable use of Lac Courte Oreilles Ojibwe College system information technology resources. System information technology resources are provided for use by currently enrolled system students, administrators, faculty, other employees, and other authorized users. The College's information technology resources are the property of Lac Courte Oreilles Ojibwe College and are provided for the direct and indirect support of the College's educational, research, service, student and campus life activities, administrative and business purposes, within the limitations of available system technology, financial and human resources. The College encourages the use of information technology as an effective and efficient tool within the framework of applicable state and federal laws, policies and rules and other necessary restrictions.

Subpart B. Academic freedom

Nothing in this procedure shall be interpreted to expand, diminish, or alter academic freedom or the terms of any charter establishing a College library as a community or public library.

Part 2. Applicability

This procedure applies to all users of system information technology, whether the user is affiliated with Lac Courte Oreilles Ojibwe College, and to all uses of those resources, wherever located. This procedure establishes minimum requirements and the College may adopt additional conditions of use for information technology resources under its control. Lac Courte Oreilles Ojibwe College is not responsible for any personal or unauthorized use of its resources, and security of data transmitted on its information technology resources cannot be guaranteed.

Part 3. Definitions

Subpart A. Security measures

Security measures means processes, software, and hardware used by College and network administrators to protect the confidentiality, integrity, and availability of the computer resources and data owned by the College or its authorized users.
Security measures may include, but are not limited to, monitoring, or reviewing individual user accounts for suspected policy violations and investigating security-related issues.

Subpart B. College information technology

College information technology means all system facilities, technologies, and information resources used for information processing, transfer, storage, and communications. This includes, but is not limited to, computer hardware and software, computer labs, classroom technologies such as computer-based instructional management systems, and computing and electronic communications devices and services, such as modems, e-mail, networks, telephones, voicemail, facsimile transmissions, video, mobile computing devices, and multimedia materials.

Subpart C. Transmit

Transmit means to send, store, collect, transfer, or otherwise alter or affect information technology resources or data contained therein.

Subpart D. User

User means any individual, including, but not limited to, students, administrators, faculty, other employees, volunteers, and other authorized individuals using college information technology in any manner, whether the user is affiliated with Lac Courte Oreilles Ojibwe College.

Part 4. Responsibilities of All Users

Subpart A. Compliance with applicable law and policy

1. Users must comply with laws, contracts, and licenses applicable to their uses. This includes, but is not limited to: the laws of libel, data privacy, copyright, trademark, gambling, obscenity, and child pornography; the Federal Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking" and similar activities; computer crime statutes; applicable conduct codes, including the Student Code of Conduct; applicable software licenses; and prohibiting discrimination and harassment, or fraudulent or other dishonest acts.
2. Users are responsible for the content of their personal use of system information technology and may be subject to liability resulting from that use.
3. Users must use only college information technology they are authorized to use and use them only in the manner and to the extent authorized. Ability to access information technology resources does not, by itself, imply authorization to do so.
4. Users are responsible for use of college information technology under their authorization.

Subpart B. Unauthorized use

Users must abide by the security restrictions on all systems and information to which access is authorized.

1. Users must not allow others who are not authorized to:
    a. use any account or password assigned by the College to anyone else;
    b. share any account or password, assigned to the user by the College, with any other individual, including family members;
    c. allow others to use college information technology under the user's control.
2. Users must not circumvent, attempt to circumvent, or assist another in circumventing security controls in place to protect the privacy and integrity of data stored on college information technology.
3. Users must not change, conceal, or forge the identification of the person using college information technology, including, but not limited to, use of e-mail.
4. Users must not knowingly download or install software onto college information technology unless allowed under applicable procedures or prior authorization has been received.
5. Users must not engage in activities that interfere with or disrupt network users, equipment, or service; intentionally distribute viruses, worms, Trojans, or other malicious code; or install software or hardware that permits unauthorized access to system information technology.
6. Users must not engage in inappropriate uses, including:
    a. Wagering or betting.

b. Activities that violate state or federal law or regulation.

c. Harassment, threats to or defamation of others, stalking, and/or discrimination.

d. Fund-raising, private business, or commercial activity, unless it is related to the mission of the College. Mission related activities are determined by the College and include activities of authorized campus or system-sponsored organizations.

e. Storage, display, transmission, or intentional or solicited receipt of material that is or may be reasonably regarded as obscene, sexually explicit, or pornographic, including any depiction, photograph, audio recording, video or written word, except as such access relates to the academic pursuits of a system student or professional activities of a College employee; and

f. "Spamming" through widespread dissemination of unsolicited and unauthorized e-mail messages.

Subpart C. Protecting privacy

Users must not violate the privacy of other users and their accounts, regardless of whether those accounts are securely protected. Technical ability to access others' accounts does not, by itself, imply authorization to do so.

Subpart D. Limitations on use

Users must avoid excessive use of college information technology, including but not limited to network capacity. Excessive use means use that is disproportionate to that of other users or is unrelated to academic or employment-related needs, or that interfere with other authorized uses. Users may be directed to limit or refrain from certain uses in accordance with this provision. The reasonableness of any specific use shall be determined by the College in the context of relevant circumstances.

Subpart E. Unauthorized representations or trademark use

Users must not use college information technology to state or imply that they speak on behalf of the College or use College trademarks or logos without prior authorization. Affiliation with the College does not, by itself, imply authorization to speak on behalf of the College.

Part 5. College Employee Users

All employees of Lac Courte Oreilles Ojibwe College are subject to the code of ethics for employees. In addition, employees are expected to use the traditional communication rules of reasonableness, respect, courtesy, and common sense when using system information technology.

Subpart A. Personal use

College employees may use system information technology for personal communications as long as the use is in accordance with state law, and the use, including the value of employee time spent, does not result in an incremental cost to the College, or results in an incremental cost that is so small as to make accounting for it unreasonable or administratively impracticable, as determined by the College.

Subpart B. Political activities

College-owned property or services, including the e-mail system, may not be used for political activities, fund-raising, or campaigning for government offices.

Subpart C. Religious activities

College employees shall not use college information technology in a manner that creates the impression that the College supports any religious group or religion generally in violation of the Establishment Clause of the First Amendment of the United States Constitution.

Part 6. Security and Privacy

Subpart A. Security

Users shall employ reasonable physical and technological security measures to protect system records in all phases of handling. This may include, but is not limited to, the appropriate use of secure facsimiles or encryption or encoding devices when electronically transmitting data that is not public.

Subpart B. Privacy.

Data transmitted via system information technology are not guaranteed to be private. Deletion of a message or file may not fully eliminate the data from the College.

Subpart C. Right to employ security measures

The College reserves the right to employ security measures, including but not limited to, the right to monitor any use of college information technology, including those used in part for personal purposes. Users have no expectation of privacy for any use of college technology resources, except as provided under federal wiretap regulations (21 U.S.C. Sections 2701-2711).

The College does not routinely monitor individual usage of its information technology resources. Normal operation and maintenance of college information technology requires the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns and other activities that are necessary for such services. When violations are suspected, appropriate steps shall be taken to investigate and take corrective action or other actions as warranted. College officials may access data on college information technology, without notice, for other business purposes including, but not limited to, retrieving business-related information; re-routing or disposing of undeliverable mail; or responding to requests for information permitted by law.

Part 7. Application of Government Records Laws

Subpart A. Data practices laws

Government data maintained on system information technology is subject to data practices laws including the federal Family Educational Rights and Privacy Act, to the same extent as they would be if kept in any other medium. Users are responsible for handling government data to which they have access or control in accordance with applicable data practices laws.

Subpart B. Records retention schedules

Official College records created or maintained electronically are subject to the data privacy requirements to the same extent as official records in any other media. Official records must be retained in accordance with the applicable approved records retention schedule appropriate for the type, nature, and content of the record. Willful improper disposal of official records may subject an employee to disciplinary action.

Part 8. College Policies and Procedures

The College must adopt policies, procedures, and guidelines consistent with this policy:

a. for breach notification or reporting possible illegal activities, users should report concerns to the Director of Information Technology;

b. the Director of Information Technology is responsible for the implementation of college security policies, procedures, and guidelines to protect the integrity of college information technology and its users' accounts;

c. the Registrar shall establish reasonable use and access procedures for handling government data in electronic form consistent with its classification under the Family Educational Rights and Privacy Act, and other applicable law or policies;

d. users should contact the Director of Information Technology to address questions, concerns, or problems regarding the use of college information technology or concerning intended or unintended interruptions of service;

e. the Dean of Institutional Advancement shall review requests to use the trademarks or logos of the College;

f. the Director of Information Technology shall provide information and education to users concerning applicable information technology policies, procedures and guidelines;

g. the Director of Information Technology shall make decisions regarding approved hardware or software use.

Part 9. Enforcement

Conduct that involves the use of college information technology resources to violate a College policy or procedure, or state or federal law, or to violate another's rights, is a serious abuse subject to limitation or termination of user privileges and appropriate disciplinary action, legal action, or both.

Subpart A. Access Limitations

Lac Courte Oreilles Ojibwe College reserves the right to temporarily restrict or prohibit use of its college information technology by any user without notice if it is determined necessary for business purposes.

Subpart B. Repeat violations of copyright laws

Lac Courte Oreilles Ojibwe College may permanently deny use of college information technology by any individual determined to be a repeat violator of copyright or other laws governing Internet use.

Subpart C. Disciplinary proceedings

Alleged violations shall be addressed through applicable college procedures, including but not limited to policies that address allegations of illegal discrimination and harassment; student conduct code for other allegations against students; or the applicable College policy for other allegations involving employees. Continued use of college information technology is a privilege subject to limitation, modification, or termination.

Subpart D. Sanctions

Willful or intentional violations of this procedure are misconduct under applicable student and employee conduct standards. Users who violate this procedure may be denied access to college information technology and may be subject to other penalties and disciplinary action, both within and outside of the College. Discipline for violations of this procedure may include any action up to and including termination or expulsion.

Subpart E. Referral to Law Enforcement

Under appropriate circumstances, Lac Courte Oreilles Ojibwe College may refer suspected violations of law to appropriate law enforcement authorities and provide access to investigative or other data as permitted by law.