	Information Technology (IT) Acceptable Use Policy

CATEGORY: IT Services	**APPROVAL DATE:** October 28, 2013
EFFECTIVE DATE: October 28, 2013	**REVIEW DATE:** July 11, 2024
APPROVAL: Cabinet (minor revision); Board of Governors	
SPONSOR: Chief Information Officer	
CONTACT: Chief Information Officer, 416-977-6000	
PREVIOUS VERSIONS: Please contact the Office of the Chief Information Officer to view previous versions	

INFORMATION TECHNOLOGY (IT) ACCEPTABLE USE POLICY 1) Purpose

The purpose of this Acceptable Use Policy (AUP) is to set forth the acceptable use of OCAD University's computing and networking facilities hereinafter referred to as the "System" and to outline what constitutes unacceptable use of the System and the consequences of violating this policy. OCAD U's System exists to support the instructional, administrative and research needs of the university. Maintenance and supervision of the System is performed by OCAD U staff to ensure User confidence in the integrity and security of this resource and to establish consistent university-wide procedures and regulations.

2) Conditions of Access and Use

Any User who has been granted access to OCAD U's networks via a User identification and password hereinafter referred to as the "User" is bound to comply with this policy.

Users are permitted to use only those accounts for which they are authorized, and shall take necessary precautions to prevent others from obtaining access to their computer accounts by keeping individual passwords confidential and by changing them regularly.

OCAD U's System are intended for university-related activities. Incidental personal use should be kept to a minimum and should neither interfere with the individual's job-related use nor with the job-related use of any university employee. Offering OCAD U networked information or services for sale or personal gain is strictly prohibited. Fundraising and advertising activities require specific authorization from the Executive Director, Advancement or Executive Director, Marketing & Communications.

Users are expected to give consideration to maximizing university resources and to proper file management. Accumulation on the network of unnecessary, out-dated, or non work related files is discouraged.

Any use of OCAD U's System to create, store or transmit material that is in violation of the Criminal Code of Canada, or the Ontario Human Rights Code or any federal, provincial or municipal laws or regulations is strictly prohibited. Users are prohibited from using the university

System in a threatening, discriminatory or harassing manner. Any use of the System that is in violation of any existing university policy is prohibited.

IT Services assumes that any data on the network is confidential and will be treated as such unless the User intentionally makes data public. Copying or examining other Users' files or programs without their consent is prohibited. Intercepting or examining the contents of messages, files or communications in transit on the network is prohibited. Entry into a university computer system, including networked systems, by individuals not specifically authorized shall be viewed as a contravention of the Trespass to Property Act and normal legal sanctions will be applicable.

Work performed by System administrators for maintenance or diagnostic purposes may at times require access to individual User files or data, however System administrators will strive to maintain the User's privacy and handle the information in an appropriate manner. In the case where a serious violation has occurred, the Chief Information Officer will report the matter to the Vice-President, Finance & Administration and to the Executive Director, People & Culture. This information will be shared with that employee's managerial supervisor and with the management of other affected services, if required.

No User shall deliberately jeopardize the integrity of the networks or computers. This includes but is not limited to: unauthorized use of another User's computer ID or password; seeking information about or attempting to modify university computer security; attempting to degrade system performance or capability; attempting to damage systems, software, intellectual property or confidential communications of others; and knowingly propagating computer viruses, electronic chain letters or spam. Users must not misrepresent their identity as senders of messages or mislead by the content of such messages. Any violation of copyright, patent, trademark, trade secret, or other intellectual property rights via the university System is prohibited. All software, in any media, is protected under the Criminal Code of Canada. Therefore, making unauthorized copies of proprietary software, or offering unauthorized copies of proprietary software to others, is prohibited by law. OCAD U assumes no liability for any breach of copyright resulting from violation of software licenses, and will assist any software supplier, with just cause, to prosecute individuals violating copyright laws.

OCAD U retains the right to remove content or communications from the university System which are in violation of this AUP.

Users will maintain the security and privacy of internal and confidential information by using IT Resources in a manner that maintains their confidentiality, integrity and availability. Users will:

1. Use the strongest authentication methods available by using secure passwords and multi-factor authentication and treat accounts, passwords and other authentication methods as confidential.
2. Use the storage methods recommended by the Information & Data Classification Policy to secure internal and confidential information.

OCAD U provided IT Resources, including computers, licensed software and the university network, are University property, and unless otherwise formally documented, are provisioned to end users as loaned or provisioned equipment or resources.

Users must:

1. Comply with IT Services instructions to return and/or replace IT Resources in your custody based on employment status, technical, cyber security, leasing or procurement obligations the University needs to address or comply with.
2. Uninstall, delete or discontinue use of OCAD University licensed software when you are no longer an active student or employee, unless instructed or authorized otherwise.

3) Complaint and violation resolution process

The Chief Information Officer may become aware of alleged violations of the AUP either through a complaint or through the course of normal operations. Confidential data will not be examined without probable cause and approval from the Executive Director, People & Culture, or delegate, and the VP, Finance & Administration to conduct the investigation. The findings of the investigation will be forwarded to the Executive Director, People & Culture to determine what further disciplinary action is required, if any. If, in the opinion of the Chief Information Officer, the integrity or security of the System is at immediate risk, the Chief Information Officer is authorized to take necessary steps to protect the System. Such steps may include the locking of an account or accounts prior to a formal investigation on an interim basis until the perceived threat has been removed.

The Chief Information Officer, upon receiving a complaint from Human Resources; from an OCAD U employee; or from any internal or external network administrator, or upon any suspicion that a violation of the AUP has occurred, will initiate a preliminary investigation. If this requires the examination of the files, programs, or passwords of individual Users, the Chief Information Officer will seek proper authorization from the Executive Director, People & Culture and the VP, Finance & Administration before proceeding.

Depending on the findings of the preliminary investigation the Chief Information Officer may take one of the following courses of action:

» if the Chief Information Officer determines there has been no violation of the AUP, then no further action will be taken other than to inform the complainants, and the Director, HR and VP, Finance & Administration of this decision.

»If the Chief Information Officer determines that the User has violated the AUP but that the offence is not intentional, serious or malicious, then the User will be informed of the decision and asked to discontinue the activities that are in violation of the AUP.

»If the User refuses to comply, the Chief Information Officer will consult with the Executive Director, People & Culture and VP, Finance & Administration to authorize to restrict the User's access while the matter is further reviewed. The decision to restore the User's account access will then reside with the VP, Finance & Administration.

»If the Chief Information Officer determines a User to be in violation of the AUP and that the offence is sufficiently serious, and/or that the User may have violated federal, provincial or municipal laws, the Chief Information Officer will refer the matter to the Executive Director, People & Culture and the VP, Finance & Administration for their recommendation as to whether the User's access should be disabled, whether further investigation needs to be conducted and/or whether the matter needs to be referred to police.