



Information Technology Acceptable Use Guidelines

All persons using Mohawk College's information technology resources and facilities (hereafter referred to as I.T. resources) must adhere to the *Information Technology Acceptable Use Guidelines*. These guidelines should be read in conjunction with the [Information Technology Security Policy](#), and the [Information Technology Code of Conduct for Student and Academic Clients](#) or the [Information Technology Code of Conduct for Employees and Contracted Individuals](#).

Guidelines for Using Personal Computers and Network Resources:

- Be familiar and comply with all federal and provincial laws, all College policies, such as the college's Human Rights policy, and the Information Technology (Student or Employee) Codes of Conduct.
- Comply with copyright laws and software licensing agreements. Software which is unauthorized or illegal may not be installed on Mohawk College servers or computers.
- Identify yourself correctly to the network when logging on, where applicable. Using someone else's account or password, or forging an account or password is strictly prohibited.
- Protect your computer, software, and files appropriately. Establish a machine (bios) password, set a password on your screen saver, and password protect sensitive or confidential data or files to prevent unauthorized users from accessing your computer, software, and files. Routine backups should also be performed to guard against the loss of information.
- Keep your accounts and passwords confidential. All users may be assigned an account and password, so there is no need to share them.
- Use College I.T. resources for college business only. Such resources may not be used for personal gain or profit, political or religious use, or commercial advertisements. Remember that all files and programs residing on a College workstation or network are the property of Mohawk College.
- Playing games, spamming of messages, broadcasting unsolicited e-mail, etc. is **an improper use of College property and a waste of valuable networking resources and is strictly prohibited.**
- Scan or ensure the necessary virus protection software is installed to scan all software and files received from others or downloaded from the internet, otherwise, you could inadvertently download, install or run any program intended to damage or place excessive loads (for example, viruses, Trojan horses, worms, etc.) on a computer system or the network. If you believe you have received a virus in an email message, for example, don't open it. Contact your LAN Administrator or the I.T. Division immediately.
- Encrypt sensitive or confidential information prior to transmitting it via the internet. Interception of data on the internet is elementary and common; therefore, College, proprietary, or private information should either be encrypted or sent via another method. This includes the transmission of credit card numbers, and log-in accounts and passwords.



Information Technology Acceptable Use Guidelines

- Make arrangements with the Director of Information Technology if you require your own personal computer equipment (including laptops), personal networking equipment (including interfaces and software), or a modem to be connected to your workstation or to the College network. Use of such equipment can degrade network performance, create security exposures and tie up needed telephone lines; therefore requests need to be reviewed for approval. Before any equipment can be installed, an **Information Technology Hardware Registration form** must be completed and submitted to the IT Director with approval by the submitter's manager.
- Contact the applicable system administrator to gain access to a particular system. Accounts and passwords are managed by those administrators only, and access cannot be granted by an unauthorized individual.
- Use internet resources for teaching, learning, research, student life, and administration purposes only. Viewing or listening to material that is illegal, offensive, or otherwise inappropriate to the user's function is prohibited.
- Remove or make arrangements to retain all personal data and files prior to leaving the College, either upon completion of a semester or graduation (students), or termination (employees). The College will remove access to all Mohawk College I.T. resources upon such leaving.
- Understand that the Information Technology Division has the right to regularly check and monitor networking resources and facilities, and reserves the right to take any appropriate action to protect such resources and facilities.

Guidelines for Using Electronic Communication Resources (e-mail and voice-mail):

- Be familiar and comply with all federal and provincial laws, all College policies, such as the college's Human Rights policy, and the Information Technology (Student or Employee) Codes of Conduct.
- Do not send or distribute messages or files of an illegal, libelous, abusive, harassing, obscene, offensive, discriminating, threatening, intimidating, or demeaning nature to any individual or group as this is strictly prohibited.
- Use College communication systems for college business only. Such resources may not be used for personal gain or profile, political or religious use, or commercial advertisements.
- Identify your official position or affiliation with Mohawk College. You may not misrepresent yourself or your intentions in any communication using College resources. Official communications must not contain information that is harmful or embarrassing to the College. Any opinions expressed by you must contain a statement that they are your opinions, and do not reflect on the College.
- Do not send or forward broadcast messages or unsolicited e-mail.
- Create an appropriate e-mail or voice-mail forwarding strategy during long periods of leave or



Information Technology Acceptable Use Guidelines

vacation. Be sure to unsubscribe from any discussion lists before you create an e-mail auto-reply message, as not doing so creates an infinite loop of messages which causes annoyance to the list owner and complaining messages for you.

- Recognize that the College cannot secure communication systems. It is therefore recommended that you do not send confidential or sensitive data or files via e-mail unless they are encrypted.
- Protect your password for your e-mail and voice-mail systems.
- Report any suspect communications to the Director of Information Technology immediately.

Guidelines for Passwords:

- Memorize your passwords. Passwords should never be written down.
- Protect your passwords from others. Never share your passwords with anyone.
- Create a password that is meaningful and easy to remember, but difficult for others to guess. It should be a minimum of six characters, preferably with numbers as well as letters. Try not to choose a password that is a proper name or a dictionary word. These are easy for hackers to decipher.
- Change your passwords every 6 to 12 months, or immediately if you suspect a hacking attempt or infiltration.
- Use a different password for each system.

Considerate and authorized use of all of Mohawk College's information technology resources and facilities will ensure suitable availability of those resources and facilities to everyone.