AP 3-705 – USE OF TECHNOLOGY

BACKGROUND

The purpose of this procedural policy is to outline the acceptable use of computer equipment at Western School Division. The procedural policy applies to all end users and to all equipment that is used within the Western School Division Network System. End users include employees, students, and guests who agree to use our network system.

General Use and Ownership

(a) All data created on the Western School Division systems remains the property of Western School Division. Because of the need to protect Western School Division's network, administration cannot guarantee the confidentiality of information stored on any network device belonging to Western School Division.
(b) End users are responsible for exercising good judgment regarding the reasonableness of personal use.
(c) For security and network maintenance purposes, authorized individuals may monitor equipment systems and network traffic at any time.
(d) Western School Division reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
(e) Should an end user wish to have a private means of accessing their personal email accounts/other communications, including any access to the internet for personal reasons, end users ought to do so utilizing their own electronic device and not through a connection to the employer's network.

Security and Proprietary Information

(a) The information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential. End users should take all necessary steps to prevent unauthorized access to information of a confidential nature.
(b) Authorized users are responsible for the security of their passwords/accounts and must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse codes.
(c) End users must exercise caution when sending any e-mail from inside Western School Division to an outside network in order to prevent the unauthorized or inadvertent disclosure of sensitive or personal information.
(d) All end users are responsible for ensuring periodic review and clean-up of their individual e-mail files to avoid undue overload on the system.

Unacceptable Use

Under no circumstances may Western School Division-owned resources be used to engage in any activity deemed illegal under provincial, federal, or international law.

Other prohibited activities include

(a) Violations of the rights of any person, organization or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations.
(b) Unauthorized copying of copyrighted material including installation of any copyrighted software for which Western School Division or the end user does not have an active license.
(c) Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
(d) Introduction of malicious programs into the network or server (eg., viruses, worms, Trojan horses, e-mail bombs, spy ware, etc.).

(e) Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
(f) Using a Western School Division computing asset to actively engage in procuring or transmitting material that is in violation with sexual harassment or hostile workplace laws in the user's local jurisdiction.
(g) Making fraudulent offers of products, items, or services originating from any Western School Division account.
(h) Making statements about commitments/guarantees, expressly or implied, unless it is a part of normal job duties.
(i) Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's host computer, via any means, locally or via the Internet/Intranet/Extranet.
(j) Providing information about, or lists of, Western School Division end users to parties outside Western School Division.

Prohibited e-mail and communications activities

(a) Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e- mail spam).
(b) Any form of harassment via e-mail, telephone or paging, whether through language, frequency, or size of messages.
(c) Unauthorized use, or forgoing, of e-mail header information.
(d) Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.
(e) Creating or forwarding "chain letters" or "pyramid" schemes of any type.
(f) Use of unsolicited e-mail originating from within Western School Division networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Western School Division or connected via Western School Division network.
(g) Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Guidelines on Anti-Virus Process

(a) Always run the Western School Division standard supported anti-virus software. Download and install anti-virus software updates as they become available (typically, this process is automated).
(b) NEVER open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
(c) Delete spam, chain, and other junk e-mail without forwarding.
(d) Never download files from unknown or suspicious sources.
(e) Avoid direct disk sharing with read/write access unless there is absolutely a requirement to do so.
(f) Always scan a USB device and external hard drive from an unknown source for viruses before using it.
(g) Back-up critical data and system configurations on a regular basis and store the data in a safe place.
(h) If the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., e-mail or file sharing.

Reference: Section 41 and 47, Public Schools Act

Adopted: August 2009
Revised: January 2013
Revised: December 2, 2020