



## AP 3-705 – USE OF TECHNOLOGY

### BACKGROUND

This procedure outlines the acceptable use of computer devices and technical equipment, *including personal electronic devices* at Western School Division. It applies to all end users. It applies to all equipment that is used within the Western School Division and to the use of the Network System of Western School Division itself. End users include employees, students, and guests. This procedure is informed in part by direction from Manitoba Education and Early Childhood Learning's, "Enhancing Guidelines for Cell Phone Use in Schools to Minimize Distractions and Support Student Learning and Safety" from August 2024.

### Use of Personal Electronic Devices by Staff, Visitors to the School and Students

#### Staff and Visitors at all Grade Levels

Western School Division staff will support students in achieving the minimization of distractions and the enhancement of student learning and safety by appropriately modelling the responsible and appropriate use of personal electronic devices when in the learning environment. As such, when on school property, a personal electronic communication device must be turned off at any time staff and visitors have contact-time with students. This includes when staff (and visitors where applicable) are in class, supervising students in school or participating in a school event. Staff must not send or receive personal communications while on the job and are responsible for the care, control, instruction or supervision of students. For staff in grades 9-12, cell phones may be used in class for educational purposes, when directed by teachers for student learning. Use of communication devices for urgent and/or emergency communications related to the safety and well-being of students, staff or visitors, is allowed at the administrator's discretion.

#### Kindergarten to Grade 8

Students may not access or use cell phones during school hours, inclusive of breaks and lunch. All communication devices must be turned off when the student enters school property. These devices may not be activated at any point during the regular school day. Students may not leave class to make or receive electronic communication (i.e.: cell phone calls, text messages or other internet communication).

#### Grades 9 to 12

Students may not use cell phones during class time. Students may be permitted to use cell phones during break times/lunch as per policies developed by the school. Students may also be permitted to use personal cell phones in class for educational purposes, *when specifically directed by classroom teachers*.

For students at all grade levels, during school outings, field trips or extra-curricular events, use of a cell phone or personal device is by permission of the supervising academic staff (principal or teacher).

#### For all Students

Any use of an electronic communication device during prohibited times or in an inappropriate manner will result in the student being required to present and relinquish their device to school staff immediately upon staff request. Devices will be returned to parents or guardians under conditions set by administration.

#### For all End Users

When determined to be necessary, the administrator can make appropriate exceptions to support medical and diverse needs. A documented plan regarding those identified needs and circumstances will be discussed and established. Cameras or phones equipped with cameras must be kept out of sight and not activated in washrooms, change rooms or any other private areas. Use of an electronic communications device or digital camera to record video, still shots or sound must be done with express permission of the supervising staff member and with full advance knowledge and permission of any individual or group being recorded. Sharing, distribution or broadcasting of any such material must be done with full permission of every individual being recorded.



Posting to the Internet may require written permission of parents. Recordings made secretly and/or used maliciously will result in disciplinary action up to and including expulsion and a police report.

### **General Use and Ownership of Divisional Technology and Networks**

Western School Division offers employees, students and other authorized users (as determined by the computer department, and school and department administrators) access to a variety of information technology resources, including computer workstations, local area networks, a wide area network and the Internet.

In response for the privilege of accessing the Internet, every Internet user has the responsibility to respect and protect the rights of every other user on the Internet, and to act in a responsible, ethical and legal manner.

**Acceptable use** of information technology includes, but is not limited to, the following:

- Use consistent with the mission of the Western School Division
- Use that encourages efficient, cooperative and creative methods to perform the user's job duties or educational tasks
- Use related to instructional, administrative and other support activities considered consistent with the mission of the Division

All educators have a responsibility to work together to help students develop the skills needed to discriminate among information sources, to identify information appropriate to student age and development levels, and to evaluate and use information to meet students' educational goals.

Electronic information research skills are fundamental to preparation of citizens and future employees who are good digital citizens. Staff will blend thoughtful use of such information throughout the curriculum and will provide guidance and instruction to students in the appropriate use of such resources.

Students are responsible for good behavior on school computer networks just as they are in a classroom or a school hallway. Communications on the network are often public in nature. General school rules for behavior and communications apply. The network is provided for students to conduct research and communicate with others and students must act in a considerate and responsible manner when using technology in schools.

Use of the Internet, Division computer networks and computer workstations is a privilege, which may be revoked at any time for abusive conduct.

It should further be noted that:

- (a) All data created on the Western School Division systems remains the property of Western School Division. Because of the need to secure, and protect Western School Division's network, administration cannot guarantee the confidentiality of information stored on any network device belonging to Western School Division.
- (b) For security and network maintenance purposes, authorized individuals may monitor equipment systems and network traffic at any time.
- (c) Western School Division reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
- (d) 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; and must do so at a time that is appropriate according to the use of personal electronic devices guidelines.



### **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, etc...

(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 (but are not limited to)**

- 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.
- 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.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate administrator/divisional authority should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan horses, e-mail bombs, spy ware, etc.).
- Using abusive language, including hate mail, harassment or discriminatory remarks
- Deliberately accessing inappropriate websites that contain obscene material, including reviewing, downloading, storing or printing files or messages that are obscene, vulgar or sexually explicit, or that use language that degrades others
- Using networks for a commercial, political or profit-making enterprise, except as specifically agreed to with the Division
- Using or accessing a file or an account owned by another user without his/her permission, or deliberately distributing or downloading any material in such a manner that causes congestion of networks
- Installing software that is not legally licensed for use. (i.e. pirated software); or Installing software that is not supplied or approved for use by the Division without authorization by an administrator
- Installing any hardware not owned by Western School Division
- 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.
- Using a Western School Division computing asset/device to actively engage in procuring or transmitting material that is in violation with any laws; or in violation of the Freedom from Violence or Freedom from Harassment administrative procedures of Western School Division.
- Making fraudulent offers of products, items, or services originating from any Western School Division account.
- 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.
- Providing information about, or lists of, Western School Division end users to parties outside Western School Division when not authorized to do so.



**Prohibited e-mail and communications activities**

- (a) Sending non-work related, unsolicited e-mail messages or other types of electronic communications, 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 electronic communication, whether through language, frequency, or size of messages.
- (c) Creating or forwarding “chain letters” or “pyramid” schemes of any type.
- (d) 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.

**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) Back-up critical data and system configurations on a regular basis and store the data in a safe place.

Reference                      Section 41 and 47, Public Schools Act

**Adopted:**                      **August 2009**  
**Revised:**                      **January 2013**  
**Revised:**                      **December 2, 2020**  
**Revised:**                      **August, 2024**