



Preparing Today's Learner for Tomorrow

Administrative Procedure 3140

Responsible Use of Information and Communication Technologies - Employees

Board Governance Policy Cross Reference: [1, 12, 13, 16](#)

Administrative Procedures Cross Reference:

[Code of Conduct](#)

[Harassment](#)

[Use of Copyright Protected Work](#)

Form Cross Reference:

Legal/Regulatory Reference:

[Manitoba Education - Literacy with ICT Across the Curriculum](#)

[The Freedom of Information and Protection of Privacy Act \(FIPPA\)](#)

The Interlake School Division (ISD) supports the responsible use of Information and Communication Technologies (ICT) in support of learning, teaching and administration. Division ICT assets include ISD owned, operated or maintained workstations, servers, printers, telephones, switches, routers, wiring and hubs; wireless and cellular components; mobile devices; tablets and laptop computers; or any ISD owned, operated or maintained technology, software, components or devices that store, process or transmit information or data.

It is the expectation of the Division that information and communication technologies are to be used in a responsible, efficient, ethical and legal manner in accordance with the Mission, Vision and Values of the Division.

The ISD supports the development of Literacy with Information and Communication Technology (LwICT) in students. This means thinking critically and creatively about information and about communication as citizens of the global community, while using ICT safely, responsibly and ethically. See [Literacy with ICT Across the Curriculum](#) for further details regarding the K-12 continuum and resources.

It is the responsibility of all staff to ensure that technology and communication tools are used to support curricular outcomes in a safe and appropriate manner. To that end, all users will learn to:

- identify material that is both age and developmentally appropriate;
- discriminate between acceptable and unacceptable information; and
- evaluate the accuracy of information available online.

All employees are required to complete an ICT Acceptable Use Agreement.

Definitions

Information and Communication Technology (ICT) resources include, but are not limited to computers, networks, internet, email, collaborative technologies and other forms of communication services and products.

Network is a wired and wireless technology network including school and division networks, cellular networks, commercial, community or home-based networks accessible to students and employees.

Devices/hardware includes, but is not limited to communication devices, smart phones, audio/video devices, computers and storage devices.

Social media is as any form of professional or personal online publication that allows interactive communication, including but not limited to, social networks, blogs, websites, internet forums and wikis. Examples of social media include but are not limited to, Facebook, Twitter, YouTube, Google, Instagram, Blogger and Flickr.

Professional social media is social media activity that is either school or school division based.

Personal social media is non-work related social media on which an individual is identifiable as an employee of the Interlake School Division.

Software is any application that is to run on divisionally owned hardware/device.

Responsible Use Guidelines:

1. The Interlake School Division's computers, software, networks, electronic communication and access to the internet are intended for educational research purposes and for conducting school or divisional business.
 - a) Personal use of divisional devices should be restricted to non-working time wherever possible (i.e. coffee breaks, lunch, evenings, weekends).
 - b) All electronic communication, both personal and business must be professional and respectful.
 - c) All electronic devices issued to staff remain the property of the Division and are to be at work with the employee every day.

2. In order to maintain system integrity and to ensure that users are utilizing the system responsibly, network administrators may, as part of their authorized responsibilities, access any divisionally owned device and network storage area at any time.
 - a) Users should not expect that there are any guarantees implied or made regarding the assurance of security, storage, or backup of personal or divisional data.
 - b) The Division will investigate, as soon as possible, instances in which it appears that its resources are being expended on content that might lack sufficient educational purpose. After consulting with the staff member who placed said content on an ISD owned device and when such content is found to lack sufficient educational purpose, corrective action may be taken.
3. The use of Division owned or employee owned devices imparts personal responsibility which encompasses the following:
 - a) Use of personally owned devices for work purposes, although encouraged for professional learning, cannot become the responsibility of the Division in terms of replacement in the event such devices are lost, damaged or stolen.
 - b) In the event that a Divisionally owned device is lost, stolen or damaged, the Division will assess financial responsibility for damages on a case by case basis.
 - c) Employees should not expect that files and communication conducted on the Division's network, computers or devices are private.
 - d) Employees must report ICT hardware, software, network or security concerns to school or division administration (or designate).
 - e) Employees must respond to a colleague's unauthorized or inappropriate use of ICT in a manner consistent with professional codes of conduct.
4. ISD staff have the right to work and learn in environments with limited distractions and where the potentially harmful impacts of cell phones and other personal devices are minimized.

In alignment with provincial guidelines and our responsibility for fostering safe, caring, respectful and inclusive schools, ISD will be implementing consistent expectations for staff use of cell phones and other personal devices across all schools:

- a) Staff use of cell phones or other personal devices during school hours will be for educational purposes that focus on teaching and learning for students in a manner consistent with professional codes of conduct.
 - i. During class time, when meeting with colleagues, or when supervising students, staff are permitted to use their cell phone or other personal devices for educational purposes only.
 - ii. During break time and lunch, staff are permitted to use their cell phone and other personal devices for non-educational purposes.

- b) Staff requiring a cell phone or other personal devices during school hours for specific educational or medical needs will be granted access by the school Principal as necessary.

5. Inappropriate use of ICT includes but is not limited to the following:

- a) Violating any local, provincial or federal laws;
- b) Violation of copyright;
- c) Accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information, copyrighted material;
- d) Selling or purchasing illegal items or substances;
- e) Obtaining and/or using unauthorized hardware or software programs;
- f) Causing harm to others or damage to their property;
- g) Using profanity or abusive language;
- h) Threatening, harassing, or making damaging or false statements about others;
- i) Deleting, copying, modifying, or forging other user's names, emails, files or data;
- j) Intentionally accessing, creating, storing or transmitting material that may be deemed to be offensive, indecent, obscene, intimidating, or hostile; or that harasses, insults or attacks others;
- k) Disguising one's identity, impersonating other users, or sending anonymous email for any reason;
- l) Damaging or altering devices, connections, files, data or the Network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance;
- m) Sharing of ISD passwords that may compromise system security;
- n) Using any Interlake School Division devices or personal devices to pursue "hacking," internal or external to Interlake School Division, or attempting to access information protected by privacy laws;
- o) Using web sites, email, networks, or other technology for political campaigning or personal gain;
- p) Advertising and/or promoting unauthorized sites or commercial efforts and events;
- q) Using the network for non-academic related bandwidth-intensive activities such as network games, transmission of large audio/video files, or using the Network to serve as a host for such activities;
- r) Using VPNs or other activities in an attempt to circumvent or bypass normal operation of the network;
- s) Using ISD owned ICT equipment for personal use (example: installation of games and software not authorized by ISD);
- t) Using ISD ICT equipment/resources to pursue a business interest or the like;
- u) Disclosing any personally identifiable information of an individual without their permission, or if individual is under the age of 18, without permission of their parent/guardian.

6. Social Media

- a) Use of professional social media sites is intended for educational and school related use only.
- b) Professional social media sites should include language that identifies the Interlake School Division, the school, course or grade level that utilizes the site.
- c) Employees should treat all social media space and communication like a classroom and/or professional workplace. The same standards expected in Interlake School Division professional settings are expected on all social media sites. If a particular type of behavior is inappropriate in the classroom or a professional workplace, then that behavior is also inappropriate on all media sites. Employees should exercise caution, sound judgment, and common sense when using social media sites.
- d) Employees should use privacy settings to control access to social media sites to ensure that all media communications only reach the employee's intended audience. However, employees should be aware that there are limitations to privacy settings. Private communication published on the internet can easily become public. Furthermore, social media sites can change their current default privacy settings and other functions. As a result, employees have an individual responsibility to understand and monitor the rules of the social media site being utilized.
- e) Social media communication should be in compliance with Interlake School Division procedures and applicable laws, including, but not limited to, prohibitions on disclosure of confidential information and prohibitions on the use of harassing, obscene, discriminatory, defamatory or threatening language.
- f) No personally identifiable student information may be posted by Division employees on any social media site, including student photographs, without consent of the students' parents or guardians.
- g) Media, including text, images, video, music, sounds, and graphics are protected under copyright laws unless the author provides permission for use without having to pay royalties. Some exceptions apply under the Fair Dealings Guidelines of the Copyright Act.
- h) Personal information and/or images of division employees or volunteers may not be posted on any social media or internet site without the prior permission of the individual concerned. In addition, employees may not "tag" or otherwise identify division employees or volunteers on social media or the internet without the prior permission of the individual being identified.
- i) Employees should not use the ISD logo in any postings or post ISD material on any personal social media sites without the permission of the school administrator.
- j) When establishing professional social media sites, school administrators and employees should consider the intended audience for the site and consider the level of privacy assigned to it, specifically, whether the site should be a private network (for example, anyone within the school or a larger group within the ISD community can participate). It is recommended practice for professional social media sites to be private networks, unless there is a specific educational need for the site to be a public network.
- k) School administrators reserve the right to remove, disable, and provide feedback regarding professional media sites that do not reasonably align with these guidelines.

7. Employees who intentionally engage in inappropriate or unauthorized use of Division computers, software, networks, electronic systems, and access to the Internet will be subject to appropriate discipline. Such discipline may include loss of computer privileges, suspension, termination of employment and/or legal action. All disciplinary action shall be subject to the relevant provisions in collective agreements.