AP 810.1: Acceptable Use of Information and Communications Technology

1. Information and Communications Technology Agreement

1.1. Users of the Board's Information and Communications Technology (ICT) will be required to agree to and sign the staff "Form 810.1a: Staff Permission for Access to Information and Communications Technology" or student "Form 810.1b: Student Permission for Access to Information and Communications Technology" as applicable.

1.2. Students under the age of 19 may have limited access if the Board receives in writing a request from their parent or legal guardian. Limited access is defined as restricting access to the Internet, e-mail, and other online services as reasonably and practically as possible and where there will be minimal impact to students' learning.

2. Access to Services

2.1. The Board will provide access to the District's communications system, which may include e-mail, social media, voice, and fax services as follows:

2.1.1. All District employees, members of the Board, students and the public will be provided access to the district's communications systems as appropriate and necessary. Public access must be authorized by the Director of Information Technology or designate. Examples of public users include contracted workers, PAC members, etc.

2.1.2. Access to conferences and features of the district's communication system may be controlled or limited based on the type of user (e.g. student, grade level, staff, public, management, etc.).

2.2. Subject to Section 2.3, if there are reasonable ground for concern, computer systems (including internet, intranet and email usage), use of social media sites, and stored items may be monitored and reviewed by the District's senior management or designate without prior notice to the user.

2.3. Users' email, files and contents shall be accessed in accordance with the requirements of the Freedom of Information and Protection of Privacy Act (FOIPPA).

3. Conduct and Expectations

3.1. It is important that users conduct themselves in a responsible, respectful and ethical manner while using the District's information and communications systems and follow the Board's Policy 310: Code of Conduct.

3.2. Use of e-mail, voice mail, and online services for personal purposes is acceptable, provided that these uses, in the opinion of the Board, do not:

3.2.1. Interfere with or detract from staff duties and responsibilities and student learning during working or classroom hours respectively

3.2.2. Compromise the integrity and efficiency of the District's information technology

facilities and services

3.3. Users will refrain from uploading and downloading copyrighted files, programs, and applications without the express permission of the owner of the material.

3.4. Due to the value and sensitive nature of some of the District's data and employee and student information, users must exercise caution and care in their work and adhere to all District policies and procedures.

3.4.1. Users are expected to protect critical or sensitive data files (softcopy and hardcopy) from accidental or intentional disclosure to unauthorized users.

3.4.2. Users must respect the privacy of other users' software and data.

3.4.3. Users should keep their access information (i.e. ID and password) to any District-owned or related systems private.

3.4.4. Users should not store confidential information on personally owned devices or storage mediums.

3.4.5. Users should not store data containing private or confidential information in non- district Internet-based services (a.k.a. "the cloud") that reside outside of Canada unless agreed to under 820: Freedom of Information and Protection of Privacy. Examples of these online services include, but is not limited to, iCloud, TeacherWeb, DropBox, etc.

3.5. Users must not maliciously attempt to harm, modify, or destroy data of another member, the Board, or any of the agencies and other networks that are connected to the Internet as well as to violate or attempt to violate the security of ICT.

3.6. The District's ICT is a shared resource and users should use it in such a way that it does not disrupt the services to others. Users must not use ICT to:

3.6.1. Send chain letters and spam

3.6.2. Play network or online games

3.6.3. Upload or download excessively large files unless required to do so for the user's work or assignment

3.6.4. Stream video content unless required to do so for the user's work or assignment

3.7. The District's ICT is not to be used for non-district commercial use. Non-district commercial use is defined as "offering or providing products or services not directly related to school district business".

3.8. The use of the District's ICT for political lobbying, fundraising or other political activities is prohibited. However, users may analyze legislative measures and communicate their constructive opinions to elected officials.

3.9. Publication of Materials

3.9.1. Personal web pages and social media accounts may provide links to web pages residing on the District's ICT or references to the District, staff and students. The Board reserves the right to require the removal of such links and references if, at the sole discretion of the Superintendent or his or her appointee, any part of personal web pages or other postings is deemed to be inappropriate or damaging to the District and its staff and students. Whenever feasible and appropriate, the Superintendent or his or her appointee will consult with his or her senior management team prior to any removal or changes.

3.9.2. School and student-produced websites, blogs, and other online materials created must:

- Relate specifically to school activities and programs or student-produced materials
- Have prior permission to use any content that has not been created by the student or the school
- Follow guidelines and policies for appropriate content as stipulated in this and other district policies
- Be approved by a sponsoring teacher if students produce the web pages
- Publication of pictures, photographs, and audio and video recordings of students must:
    - Not contain personal information such as addresses, phone numbers, the full names of students (use of first names is acceptable).
    - Have the express permission by the students' parent or guardian to publish the media containing their child's image or recording.

3.9.3. Advertisements and promotion of events must be directly related to the District and must be authorized by a District administrator or the Board.

3.9.4. Posting materials on social media sites such as on YouTube, Facebook, Twitter etc. should follow the same regulations and guidelines as for publishing materials via other means.

- Users should consider anything that is published to a social media site would be public and permanent; therefore, users should exercise discretion before posting anything. Users should be aware that they might be directly liable for inappropriate postings on the Internet that could include, but is not limited to, appropriate disciplinary actions and the involvement of law enforcement authorities.
- Staff that use social media to interact with students and parents via social media sites should follow these procedures:

- Separate their personal social media accounts with their social media work accounts – Set one or more personal and one or more for interacting with students/parents (e.g. one for current students and one for former students)
- Do not "friend" students on your personal accounts
- For staffs' and students' protection, personal "chatting" with students is highly discouraged. For general discussions, students should post their comments on a publicly viewable "wall" or blog
- Where applicable, create group/classroom areas or accounts for students to post and share information and materials
- Model safe and responsible behaviour and actions. Learn and instruct students on controlling privacy and social responsibilities.

- Students that use social media:
  - May use it as part of supporting their learning during class time.
  - Should conduct themselves appropriately at all times. It is recognized that the line between personal and classroom use is not always clear.
  - Should refrain from posting photos and videos that can potentially be damaging to themselves or to others or causing authorities to be involved
  - Should use privacy settings to limit the public accessibility of their information and images

4. Overall Responsibilities

4.1. The Director of Information Technology shall be responsible for the overall system coordination and relationships with regional or provincial programs.

4.2. Reasonable measures will be taken to supervise students while they are using the Internet. However, the School District and its employees cannot be responsible for direct and continual supervision of every student while they are using the Internet.

4.3. Procedures for ICT users who intentionally modify or tamper with ICT equipment without prior authorization are found in Section 11.

5. Responsibilities of ICT Administration and Staff

5.1. The Director of Information Technology or designate shall be responsible for assigning responsibility to District staff to maintain and monitor the District's ICT.

5.2. Like all other employees of the District, staff who support the information technology infrastructure and provide information technology services are expected in the normal course of business to use information technology appropriately, respect the privacy of others, and maintain the confidentiality of information that may come to their attention during the routine exercise of their duties.

5.3. Information technology employees will ascertain and release information that is normally confidential only when specifically requested to do so according to the provisions of Section 2 of this Policy.

5.4. In situations where there is an immediate threat to the integrity and availability of the District's networks and data systems, ICT management have the obligation and authority to take the measures that they, in their professional judgment, think are necessary to secure the networks and systems for general use, even if this means denying access and causing loss or inconvenience to some users. ICT staff has the responsibility to report to ICT management of concerns they may have in regards to the integrity and availability of the District's networks and data system.

6. Responsibilities to Building-Level Administrators

6.1. The Building-Level Administrator for schools shall be the school principal. For other facilities, the designated building manager for each facility shall be the Building-Level Administrator.

6.2. Administrators will ensure that all of the employees under their supervision receive instruction of this policy and that they are followed.

6.3. School administrators will establish a process to ensure adequate supervision and safety of students using ICT.

6.4. Administrators, in consultation with their supervisor, are responsible for conducting building-level activities such as maintaining and reviewing school, department, and staff web pages and applying this policy at the building level. Administrators may designate another staff member the upkeep of the school's or department's website as appropriate.

7. Responsibilities of Teachers and Student Supervisory Staff

7.1. Teachers and other adults who directly supervise students shall be responsible for educating students about the acceptable, safe, and socially responsible uses and by providing general supervision and enforcing this Policy.

8. Responsibilities of Parents

8.1. Parents are responsible for ensuring that they fully understand the terms and conditions of this policy and have discussed this with their children that attend school in School District 8 - Kootenay Lake.

9. Responsibilities of All ICT Users

9.1. All ICT users are expected to be familiar with and comply with Policy 810: Use of Information and Communications Technology, this guideline and the related ICT

Acceptable Use Agreement.

9.2. All ICT users are expected to use technology responsibly out of district as it relates to the impact it may have on the District.

9.3. All ICT users should report to their supervisor or, in the case of students, their teacher all suspected illegal or unacceptable use of ICT resources.

10. Modifications of Information and Communication Technology

10.1. The modification or alteration of the District's ICT are to be performed by designated employees. This includes:

10.1.1. *Network infrastructure*
The Network Infrastructure covers both the LAN (local area network) and the WAN (wide area network, "PLNet", or "NGN") and all devices that facilitate the connections of computers and peripherals on the network. Other than the Information Technology Department (IT), no staff member, or member of the public is permitted to make any modifications to any network device regardless of location. This includes disconnecting and replacing cables. Unauthorized changes to networks may result in the disconnection or deactivation of that portion of the network if it is determined that the alteration is causing or may cause safety concerns or problems for the network.

10.1.2. *Telephones, photocopiers, printers*
IT department staff are authorized to move these devices. Network cables attached to these devices must not be disconnected, moved, or switched by non-IT staff.

10.1.3. *Hardware repairs/modifications*
Other than the IT Department, no staff member or member of the public is permitted to perform any modification to a computer device that is to be maintained and supported by the District. The repair and labour costs resulting from any device altered or modified by an unauthorized person may result in costs incurred to the school or department. The Director of IT may authorize temporary limited modifications.

10.1.4. *Servers*
All servers are the sole responsibility of the IT Department to maintain, administer, and support.

10.1.5. *Computer workstations including Laptops*
Any workstation that has been imaged to a District Standard will be maintained by the IT Department and cannot be modified unless it has been designated as a Lab Teacher Workstation. In these cases, the teacher will have access rights to install and test different devices and software for the purposes of instructional software testing. Should any of these Lab Teacher Workstations require a rebuild of the software, the IT Department will re-image back to the District Standard. It will be the responsibility of the teacher to install any additional applications.

10.1.6. *Mobile telephones*
Board-provided mobile telephones may be supplied with pre-configured settings and software. Users may customize their district-supplied mobile telephones to suit their particular needs. However, users are solely responsible for saving and backing up any additional content that are added. Mobile telephones that are repaired, updated or replaced may be supplied back to users without their customized data and programs.

10.1.7. *Portable computing devices*
Board-provided portable computing devices not included in 10.1.5 above might be supplied with pre-configured settings and software. Users may customize these devices to suit their particular needs in accordance to direction given by school or district management.
However, users will be responsible for saving and backing up any additional content that is added. Portable computing devices that are repaired, updated or replaced may be supplied back to users without their data and user-installed programs.

10.2. Costs to repair, restore, or rectify unauthorized modifications will be at the responsibility of the department or site of where the equipment is located.

11. Breach of Policy

11.1. Breach of this policy and procedures may result in disciplinary actions in accordance to Board or local school practices as applicable, as well as potential legal actions.

11.2. Unauthorized modifications of District information and communication technology will follow the procedures described in the following diagram.

Procedure for Handling Unauthorized Modifications to District ICT