Administrative Guidelines

Adopted: 03 July 2012
Revised: 26 November 2015; 01 February 2018

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 information security and privacy 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. Examples of these online services include, but is not limited to, GoogleDocs, iCloud, TeacherWeb, DropBox, etc.

3.5. Users must not maliciously attempt to harm, modify, or destroy data of another

3.8. The use of the District's ICS 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 ICS 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

Administrative Guidelines

Adopted: 03 July 2012
Revised: 26 November 2015; 01 February 2018

5.4. In situations where there is an immediate threat to the integrity and availability of the District's networks and data systems, ICS 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. ICS staff has the responsibility to report to ICS management of concerns they may have in regards to the integrity and availability of the District's networks and data system.

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 ICS.

Adopted: 03 July 2012
Revised: 26 November 2015; 01 February 2018

Administrative Guidelines

Adopted: 03 July 2012
Revised: 26 November 2015; 01 February 2018

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.

Adopted: 03 July 2012
Revised: 26 November 2015; 01 February 2018

Adopted: 03 July 2012
Revised: 26 November 2015; 01 February 2018