Administrative Procedures Manual	Administrative Procedure 140 Technology and Network Responsible Use
	APPROVED: September 1, 2013
Page 1 of 6	AMENDED/REVIEWED: August 2020, September 2019, January 2019
LEGAL REFERENCE:	Section 31, 52, 53, 196, 197, 222 Education Act Freedom of Information and Protection of Privacy Act Canadian Charter of Rights and Freedoms Canadian Criminal Code Copyright Act ATA Code of Professional Conduct

Background

The use of computers, telecommunications and network services provides increased access to learning opportunities with the potential to improve student achievement. Furthermore, it provides staff and students with access to the technologies to enhance their contributions to the Division's mandate and functions. The Division endorses teaching, learning and communication practices that utilize computer networks, Internet access and other electronic resources.

The purpose of providing access to networked services and the Internet is to promote educational excellence by:

- Increasing the availability of technology-based resources
- Facilitating communication in support of research and education
- Providing staff, students and approved community members with opportunities to develop computer literacy skills

Definitions

Responsible Use is defined as a responsibility of each user of Division or school computer networks to ensure that such use:

- Supports educational activities and communications consistent with the Division's mission and goals
- Complies with the computer network security requirements of the Division

Irresponsible Use includes, but is not limited to, activities that do not meet the following Responsible Use criteria:

- Committing illegal or unethical acts, including any use of the network / computer to plan or carry out acts of fraud, theft, harassment or vandalism, or to damage or destroy applications or data or any information necessary to operate the Division
- Transmitting, or gaining access to any material that breaks copyright or material protected by trade secret, or committing plagiarism of information or violating an individual's personal privacy
- Transmitting, or gaining access to obscene or threatening material, written or pictorial, including, but not restricted to, material (except where authorized by school administration or teaching staff in relation to approved curricular activities) which contains or promotes pornography, racial supremacy, ethnic hatred, or violation of human rights

- Using Division networks for unauthorized commercial activities by for-profit organizations
- Using Division networks for unauthorized product advertisement
- Placing unlawful material on a computer system within, or accessed by, the Division network
- Conducting activities that are wasteful of network resources or that degrade or disrupt network performance, including other networks and systems accessed on the Internet
- Sending messages that include profanity, vulgarities, or any other inappropriate language, including sexual, racial, religious or ethnic slurs, or any abusive, threatening or otherwise offensive language
- Revealing over the network, without consent from the person(s) affected, any personal addresses, phone numbers or identifying information of other persons or otherwise invading their privacy
- Breaking confidentiality of any account or password or making them accessible to others
- Attempting to login as either another user or as a system administrator without permission from authorized school or Division network officials

Vandalism is defined as any malicious attempt to harm, modify, or destroy data of another user, a wide or local area network, the Internet, or other networks. This includes, but is not limited to:

- The uploading or creating of computer viruses
- Any malware (viruses)
- Keystroke recording or Trojan programs

Harassment in the network context is defined as the persistent annoyance of another user, or the interference of another user's work. Harassment includes, but is not limited to, the sending of unwanted mail and placing files in another user's storage areas.

Procedures

1. The use of computers, computer networks, the Internet and information services is a privilege, not a right, and irresponsible use may result in cancellation of that privilege for any user, whether that user is a student, a Division staff member or a community member.

2. The Superintendent will ensure that procedures are in place to control student access to offensive materials but it is ultimately the parent's responsibility for setting and conveying the standards that his/her child is to follow when using media and information sources.

3. Access to Division computers, computer networks, the Internet and information services will be provided to students, staff and approved community members who agree to practice responsible use and agree to the terms and conditions established in school and Division procedures.

4. The Principal, in cooperation with school staff, shall:

   4.1 Ensure that all of the employees at that location receive instruction in the Division network procedures

   4.2 Ensure that students shall not be granted access to the Division network until they and/or their parents/guardians complete a responsible user agreement with the school or Division

   4.3 Maintain a record of user agreements in student records

   4.4 Submit completed staff user agreements to the Human Resources Department for filing

   4.5 Establish procedures to ensure adequate supervision of students using the network

   4.6 Ensure that information about Division network procedures is provided to all authorized users

5. Responsible Use Agreements

   5.1 (Form 140-1) Student Responsible Use of Technology Form,
   (Form 140-2) Staff Responsible Use of Technology Form, or
   (Form 140-3) Community Members Responsible Use of Technology Form, must be signed by the respective parties prior to the use of Division computers and the Division network.
   (Form 140-4) Contractor Responsible Use of Technology Form, must be signed by the respective parties prior to the use of Division computers and the Division network.

   5.2 Failure to sign a Computer Network Responsible Use Agreement in the prescribed form will result in a failure to obtain or loss of access to Division computers and/or the Division's computer network, the Internet and information services.

   5.3 Principals and staff shall ensure that all students registered in their school have signed a user agreement to authorize their access to the network.

5.3.1 Written parent/guardian permission is required for students under the age of eighteen (18) years unless the student has been designated an "independent student".

5.3.2 Adult and designated independent students may sign agreements for themselves.

5.3.3 In circumstances where a student user agreement has not been returned by the parent authorizing the student's use and where this will negatively impact the students learning, the Principal may sign the user agreement on behalf of the parent provided the Principal believes such approval would be acceptable to the parent and that the user agreement has been reviewed with the student. In such a case, a copy of the signed user agreement shall be mailed to the parent for their information.

5.3.4 Students with diverse learning needs may be exempted from signing an agreement at the discretion of the Principal.

5.4 All staff members must complete a user agreement in order to be authorized to access and utilize the computer network. Completed user agreements are to be submitted to the Human Resources Department for placement on employee records.

5.5 Where a community training program is to be conducted at a Division computer workstation(s), the Principal/site supervisor may authorize such use when satisfied that the network security is ensured.

5.6 Suspected abuses are to be reported to the Superintendent or designate.

6. Violations of Responsible Use

6.1 Any user violating these Procedures, or any applicable provincial, federal or international laws, or posted classroom, school or Division rules, is subject to loss of computer and Internet privileges and any other disciplinary options provided within the Education Act and/or Division procedures.

6.2 Each Principal shall have the sole discretion, at school level, in determining what is responsible use of the network, in consultation with the school community, so long as the use is consistent with Division procedures.

6.3 The Superintendent or designate has the authority to provide interpretation of what constitutes responsible use. Criteria to be used in assessing the severity of violation may include, but is not restricted to:

6.3.1 The nature of the violation

6.3.2 Whether or not students had access to the material

6.3.3 The time of day when access occurred (i.e. was it disruptive to work/learning time)

6.3.4 Frequency (i.e. one (1) time only; frequent and consistent over time)

6.3.5 Whether Division or personal equipment was being used

6.4 In such matters as expulsion hearings or where appeals are made by parents or students sixteen (16) years of age or over, the Board may also determine what constitutes responsible use.

7. Monitoring Network Use and Responsibility for Irresponsible Material Access

7.1 The Superintendent or designate, may review or cause to be reviewed any material on students, staff or community member accounts and files to monitor file server space and/or to make determination on whether specific uses of the network are responsible.

7.2 It is the user's responsibility to not initiate access to irresponsible material and to cease access to such material immediately upon discovery that access has been inadvertently gained to such material.

7.3 The Division acknowledges that it is impossible to completely control the content of data that a user may discover or encounter through use of the Internet; however, the Superintendent or designate, may authorize the application of software programs to restrict or track access to inappropriate material.

7.4 Division staff will endeavour to provide reasonable levels of supervision of computer network access, although it may not be practical to provide direct supervision of each student, staff member, or community member in every circumstance in which he or she is using computers or networked services.

8. Liability of the Division

8.1 The Division makes no guarantee of any kind, whether expressed or implied, of the service it is providing.

8.1.1 Without limiting the generality of the foregoing, this includes loss of data resulting from delays, error or omissions.

8.2 Use of any information obtained via the Internet is at one's own risk.

8.3 The Division specifically denies responsibility for the accuracy or quality of information obtained through this service.

9. Network Security

9.1 Users are to protect their unique personal passwords and keep them private to ensure system security. Passwords are to be changed periodically.

9.1.1 Users of the SRB HR/Financial System are assigned permanent user names and passwords which can only be changed by the SRB Administrator.

9.2 The Superintendent or designate, shall ensure that an appropriate password standard exists within the Division to protect the Division computers and network services.

9.3 It is irresponsible for any user to attempt to login as either another user or as a system administrator without permission from authorized school or Division network officials.

9.4 Vandalism of computer or network equipment, software or data files, including theft or unauthorized entry, and/or harassment of any user or any user's files will not be tolerated.

9.5 All computer records, including but not limited to electronic communication related to the Division's mandate and function may be accessed by the Superintendent or designate.

9.6 Users have limited privacy expectations in the contents of their files and records of their online activity while using the Division's computer network.

9.7 The Director of Information Technology shall ensure appropriate audit procedures exist for all Division computer and network systems.