	Chinook's Edge School Division – Administrative Procedure
	AP 2 – 20 Technology Access
Related Policies:	**Initial Approval:** 2012 September 18
Related Procedures: *AP 3 – 15 Student Suspension/Expulsion*	**Last Amended: 2021 January 8**
Exhibits: *Technology Responsible Use Terms and Conditions*	**Last Reviewed: 2021 January 8**

PURPOSE

The Division believes that data networks are valuable educational tools and encourages the use of data technology and networks in Division schools.

The Division has invested considerable funds in network facilities and resources, and expects employees and students to use Division technology devices and network accounts in a legal, responsible, ethical, and appropriate manner. The Division expects employees and students to use Division technology and accounts in a manner that respects the rights of all users, including their right to privacy, and to be free from harassment or interference with their use of the technology.

The Division's technology services shall be used for educational purposes or for activities that support the education of students. The Board encourages students and employees to use the data networks to locate, use, and exchange information and ideas that enhance the educational process and adhere to the rules for acceptable conduct and responsible use of educational resources in the school.

The Division approves of appropriate disciplinary action whenever students or employees engage in activities that are contrary to this policy. The Division limits the use of Division-owned network accounts by employees and students to the uses specifically agreed to and accepted by the employees and students prior to issuing access privileges in the Appropriate Use Agreement.

The Division believes that parents and guardians are ultimately responsible for setting and conveying the standards that their children should follow when using information sources. The Board respects each student's and parent's right to decide whether or not to apply for access.

PROCEDURES

1. As a condition of access to Division technology services and facilities, a user shall abide by the following:
   - 1.1. Adhere to the Appropriate Use Agreement; in the case of students under 18 years of age, the student's parent shall also consent to adherence as part of the student registration process.
   - 1.2. Appropriate Use includes:
     - 1.2.1. using only network accounts or technology services that have been authorized for their use by the teacher or Principal;
     - 1.2.2. using technology services only for educational, research, and administrative services;
     - 1.2.3. protecting one's personal access code / password and taking precautions against others obtaining access to their technology resources;
     - 1.2.4. respecting the rights of other users of the services, particularly regarding security of access and confidentiality of data.
   - 1.3. Inappropriate Use includes:
     - 1.3.1. violating the Criminal Code of Canada. The following are illegal: possessing or publishing obscene material, child pornography, blasphemous libel (swearing),
     - 1.3.2. defamatory libel (intentionally false communication that injures another person's reputation), statements intended to incite hatred of an identifiable group; gaining illegal

entry into other computer networks (hacking); or using another's technology access to access services (theft);

1.3.3. violating the Copyright Act including: unauthorized duplication of software and reproducing materials for publication without the permission of the author;

1.3.4. interfering with or disrupting computer systems by introducing viruses;

1.3.5. unauthorized use of software outside of a software licensing agreement;

1.3.6. harassing, insulting or attacking other users;

1.3.7. using other people's access codes. The sharing of access codes or passwords is prohibited;

1.3.8. trespassing into other people's technology / data records;

1.3.9. damaging technology, systems, or networks;

1.3.10. using CESD accounts and facilities for commercial purposes or monetary gain unless permission has been obtained from the Superintendent for activities that will be of benefit to the educational community;

1.3.11. taking programs or data owned by the Division to other sites without permission;

1.3.12. encroaching on the use of technology resources by others by excessive game playing, chatting, or sending chain letters; and

1.3.13. making unauthorized purchases through data networks.

1.4. Written permission must be sought from parents prior to the publication of student work on the internet.

1.5. No pictures identifying students, names of students, or personal information is to be published on the internet without appropriate consent and approval.

2. Audits

Division employees may conduct an audit of any computer equipment, files, and documents stored on equipment owned or managed by the Board or any school to determine breaches of the acceptable use policy and/or the Agreement.

Random audits may be conducted of Internet sites accessed and the contents of student folders, including subdirectories of students, staff, and anyone using the division technology system.

Those employees responsible for the use of the technology systems must, in the normal course of business, have access to all files. The Superintendent may authorize examination of specific files. Such an examination shall be accompanied by notification to the originator of such files and the reason for examination.

3. Reporting

Students and employees have a duty to report to the teacher in charge or their immediate supervisor the following:

3.1. any violations of the use of the network; or

3.2. identification of a security problem on the network.

4. Disciplinary Action

If a teacher or a Principal or other Board employee has reasonable suspicion of a violation of this policy or the Agreement entered into for use,

4.1. the employee shall report the suspected violation to his/her immediate supervisor with

4.1.1. a description of the nature of the violation; and

4.1.2. supporting evidence of the violation.

4.2. the supervisor shall inform the user that an audit of his/her computer files has been undertaken and the reasons for the audit will be given.

4.3. if there is sufficient evidence that the agreement has been broken by the user, the supervisor may

4.3.1. issue a written reprimand;
4.3.2. modify or suspend technology access privileges;
4.3.3. suspend or recommend expulsion (in the case of a student); or
4.3.4. report the circumstances to the Superintendent (in the case of an employee); or
4.3.5. report illegal activities to the police; and
4.3.6. remove files.

4.4. suspension and expulsion procedures shall be subject to the process set out in the Board's *Administrative Procedure 3–15 / Student Suspension/Expulsion*.

REFERENCE AND LINKS

Canadian Charter of Rights and Freedoms
Canadian Criminal Code
Education Act

HISTORY

2013 Oct 15 Reviewed
2019 Nov 26 Reviewed
2021 Jan 8 Revised