RESPONSIBLE NETWORK USE

Background

The Division has made provisions for the use of technology by students and staff to enhance learning opportunities. Use of Division provided technology is a privilege and it is expected that users will take advantage of this privilege in a responsible manner.

Procedures

1. PRSDnet users are responsible for their behaviour on school computer networks just as they are in the classroom or school hallway.
   - 1.1 Communications on the network are often public in nature.
   - 1.2 General school rules for behaviour and communications apply to network use.
   - 1.3 Violation of PRSDnet responsibilities will result in a loss of access and may result in other legal or disciplinary actions. For students, Administrative Procedures 350 – Student Conduct and 355 – Student Discipline apply.

2. PRSDnet is provided for staff and students to conduct research and communication with others in relation to school work and operations.
   - 2.1 Access to network services is given to users who agree to act in a considerate and responsible manner.
   - 2.2 All users must sign or agree to a PRSDnet Responsible Use Agreement (Student Form 140-1, Staff Form 140-2) prior to use of PRSDnet. For students, parent/guardian permission is required. Access is a privilege, not a right.
   - 2.3 Inappropriate use is not permitted and shall not be tolerated.
   - 2.4 Either the school designated or Division network administrators may temporarily close an account at any time.
   - 2.5 Upon review Division administration and staff may limit or suspend specific user accounts.

3. Individual users of PRSDnet are responsible for their use of the network.
   - 3.1 The use of their account must be in support of education and research and must be consistent with academic expectations of the Division.
   - 3.2 Use of other organizations' networks or computing resources must comply with the rules appropriate for that network.
   - 3.3 Transmission of any material in violation of Canadian or Alberta laws, including copyright, threatening or obscene materials, is prohibited.
   - 3.4 Use for unauthorized commercial activities by for-profit organizations, product

promotion, or illegal activities are strictly prohibited.

4. The user is expected to observe the following network procedures:
   - 4.1 Keep personal passwords, personal address and phone numbers confidential.
   - 4.2 Respect the confidentiality of others passwords, personal addresses and phone numbers of others.
   - 4.3 Use the network in such a way that will not disrupt the use of the network by other users.
   - 4.4 Treat others' data with respect: do not attempt to modify, or harm the data of another user.
   - 4.5 Copyright must be respected.
   - 4.6 Use the network to access authorized networks or computer systems.
   - 4.7 Seeking, transmitting or accepting obscene materials is prohibited.
   - 4.8 Use electronic mail with care and in accordance with Administrative Procedure 140 Appendix – Electronic Mail, recognizing that it is not necessarily private.
   - 4.9 Refrain from the use of profanity, racist comments, harassment, obscene language or other language or dialog that is offensive.

5. No Expectation of Privacy
   - 5.1 The computers and computer accounts given to users are to assist them in performance of their work within the school setting.
   - 5.2 Users are not to have an expectation of privacy in anything they create, store, send, or receive on the computer system.

6. Waste of Computer Resources
   - 6.1 Users may not deliberately perform acts that waste computer resource or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to:
     - 6.1.1 Sending mass mailings or chain letters,
     - 6.1.2 Downloading or transmitting large files,
     - 6.1.3 Printing multiple copies of documents, or
     - 6.1.4 Otherwise creating unnecessary network traffic.

7. Misuse of Software
   - 7.1 Without prior written authorization from the Technology Services Manager users may not do any of the following:
     - 7.1.1 Copy software for use on their home computers;
     - 7.1.2 Provide copies of software to any independent contractors or clients of the Division or to any third person;
     - 7.1.3 Install software on any of the Division's workstations or servers without an

appropriate license to use the software;

7.1.4 Modify, revise, transform, recast, or adapt any software; or

7.1.5 Reverse-engineer, disassemble, or decompile any software.

7.2 Users who become aware of any misuse of software or violation of copyright are to immediately report the incident to the Technology Services Manager.

8. Use of Encryption Software

8.1 Users may not install or use encryption software (except if required in the execution of their work duties) on any Division owned devices without first obtaining permission from their supervisors.

8.2 Users may not use passwords or encryption keys on Division owned devices that are unknown to the Technology Services Manager.

9. Freedom of Information and Protection of Privacy (FOIP)

9.1 If the user is not sure whether the information transmitted, received or otherwise is a "record" under FOIP, or if the information can be disclosed under FOIP, the user is to contact the Division's FOIP Coordinator relative to the proper use of the information.

Adopted/Revised: JUN 2016/NOV 2019/JUL 2021

Reference: Section 12, 18, 20, 45, 45.1, 60, 61, 113 Education Act
Freedom of Information and Protection of Privacy Act
Canadian Charter of Rights and Freedoms
Canadian Criminal Code
Copyright Act
I.T.I.L. Standards, Alberta Education
ATA Code of Professional Conduct