AP 620 NETWORK ACCEPTABLE USE
POLICY 620

CARIBOO - CHILCOTIN SCHOOL DISTRICT

RATIONALE:

The school district has guidelines and expectations for every employee regarding their use of information technology and online communications. The district is committed within available resources to providing reliable and secure online systems and resources for the purpose of learning, teaching and the management and administration of district operations.

1. Definitions:

1.1 District Electronic Resources:

All hardware (computers, printers, scanners, and other peripheral devices) as well as related software

1.2 District Network:

Is comprised of school LANs (local area network), administrative offices, and the district WAN (wide area network)

The District network is set up and maintained by the District Technology Department to allow communication, using computers and other devices, between District Offices and District Schools. The District Network is connected to the Provincial Learning Network (PLNet). PLNet is a secure, high-speed connection to government, the Internet, and educational programs. There is a secure corporate network for District issued devices and a guest network for visitors.

1.3 District Network Accounts:

Allows access to the District network, including the Internet, email, and related resources.

1.4 Personal Electronic Devices and Accounts:

Any personal technical device, such as cell phones, tablets, laptop computers, peripherals, video games or related hardware and/or software as well as personal email and social media accounts.

2. Procedures:

Prior to allowing access to the District network, each school or site will clearly communicate with students, parents, and staff the purposes, benefits, and risks associated with the use of this resource.

2.1 The Principal, or his or her designate, shall ensure that Acceptable Use forms are signed by the student and his/her parents or guardians in accordance with board policy. These forms will be kept on file at the school.

2.2 All employees must sign a District Network Usage Agreement form at the time of hiring. The administrator/Principal of each site should annually review this form with staff.

3. Alerts:

3.1 All District network accounts and folders may be examined by School District technology staff without notice to the account holder to ensure compliance with board policy.

3.2 All emails, both incoming and outgoing, may be examined at any time by the school/District to ensure compliance with board policy.

3.3 No student shall have access to the school computer network unless authorized by a teacher or other designated staff members.

4. Access to the SD27 Network:

The use of the District computer network resources is a privilege, not a right. Inappropriate use may result in the loss of this privilege and, depending on the nature of the offence, further action may occur including, but not limited to, notification of the RCMP.

4.1 The Technology Department or school Principal will determine what is deemed inappropriate use as per the guidelines - clause 5 and report the infraction to the appropriate supervisor for action.

4.2 Employees may use the District network outside of scheduled hours of work, provided that such use is consistent with professional conduct and is not used for business purposes.

5. The Use of SD27 Network Resources:

Use of the network should be consistent with the educational objectives of SD 27 and used in ways that comply with the intent of this Policy and legal and ethical standards.

5.1 Unacceptable personal use includes, but is not limited to:

5.1.1 Intentional access to sites which contain information that is pornographic, racist, sexist, malicious, vulgar, immoral, or promotes or fosters hatred or illegal activities as well as any other sites that are prohibited by the school administration and/or School District;

5.1.2 Downloading and/or installing movies, games, music files, and/or software for personal use (i.e., it must be for an educational purpose);

5.1.3 Using the District network resources for commercial or financial gain;

5.1.4 Sending or displaying offensive messages or pictures;

5.1.5 Using impolite, abusive, or obscene language;

5.1.6 Harassing, insulting, or attacking others;

5.1.7 Accessing unauthorized computer systems, folders, and files;

5.1.8 Damaging computer systems or networks by the spreading of computer malware;

5.1.9 Physically damaging computer systems, network equipment or peripheral devices;

5.1.10 Installing non-approved software applications including Peer to Peer programs (file-sharing solutions outside of the district network);

5.1.11 Students ordering or purchasing personal items online.

Given the ongoing changes to technology and technical resources, it is clear that the School District is unable to identify all current or future unacceptable uses of the District Network. Therefore, the School District reserves the right to add to this list of unacceptable uses as circumstances arise. Users cannot assume that if something is not included on the above list, it is permissible.

5.2 All account holders shall make the security of the network a priority.

5.2.1 The individual account holder is responsible at all times for its proper use and will be held accountable for any misuse;

5.2.2 If an account holder's password is known to anyone else, or if there is a reason to suspect that someone has access to his/her password, the user must change their password immediately. If there is reason to believe the account has been used inappropriately, the school administration or supervisor must be informed;

5.2.3 Use of network accounts by anyone other than the registered account owner is prohibited. If someone other than the registered user is using an account, both the unauthorized user and the registered owner may have his/her accounts disabled, and his/her computer/network privileges suspended;

5.2.4 To attempt to access any computer, network, system, software program, or data file to which the account holder does not have authorization, is strictly prohibited, and will lead to immediate revocation of computer privileges;

5.2.5 The use of any administration login and password is strictly prohibited and will lead to immediate revocation of computer privileges. If a user is aware of other users knowing any of these passwords, he/she must report this to the school administration immediately;

5.2.6 Users shall ensure they have logged off / locked / shutdown computers when leaving unattended.

5.3 When using any email program, users must follow proper email etiquette (see b. below).

5.3.1 General comments:

5.3.1.1 All email communication is to be of a professional nature;

5.3.1.2 Use of profane, harassing, or otherwise inappropriate language is forbidden.

5.3.2 Proper etiquette includes:

5.3.2.1 Messages which are respectful in nature and appropriate in content whether the communication is between students, between staff members or between students and staff;

5.3.2.2 Messages whose language is of the same standard as other forms of communication used within the school setting.

5.3.4 Users must not:

5.3.4.1 Access another user's email without his/her permission;

5.3.4.2 Create and/or forward chain letters or other unsolicited or unwanted messages;

5.3.4.3 Create and/or send email with the purport to come from another individual (commonly known as "spoofing"), or otherwise assuming an anonymous or false identity in communicating with other individuals, businesses, or organizations;

5.3.4.4 Participate in, or subscribe to non-school district related mailing lists, newsgroups, chat services, electronic bulletin boards, or any other association or service which would cause a large number of emails or other electronic messages to be sent through the District's computer network.

5.3.4.5 Reporting of suspicious email (phishing) to the IT Department.

5.4 **Transmission or use of any material that is in violation of Canadian or Provincial laws, or of School, or School District Policy, is prohibited and will be reported to the appropriate school or law enforcement agency.**

5.4.1 Use or transmission of inappropriate material constitutes grounds for termination of all computer/network access;

5.4.2 Inappropriate transmissions include, but are not limited to:

5.4.2.1 Unauthorized copying, reproduction, downloading, use or transmission of files, programs, data, documents, or information protected by copyright, trademark, trade secret, or by licensing agreements, user agreements, or similar contracts. (this includes the downloading of illegal music files, games, and other software programs, and the duplicating/burning of CDs and DVD's);

5.4.2.2 The downloading, copying, reproduction, or transmission of threatening or obscene materials or materials demonstrating antisocial behaviors or activities;

5.4.2.3 The transmission of materials associated with commercial activities;

5.4.2.4 The transmission of materials/messages relating to or in support of illegal activities;

5.4.2.5 The use or transmission of materials used for political lobbying.

5.5 Use of personal electronic devices:

5.5.1 Personal Devices (BYOD) can be used to access the provided BYOD wireless network;

5.5.2 Cell phones, tablets and other personal devices are not to be used during instructional time unless they are part of the instructional program.

5.5.3 Schools may have rules or guidelines which limit the use of personal devices during the instructional day;

5.5.4 Infractions of the above will be dealt with as appropriate.

6. Internet and Email Safety

The District's primary concern when providing Internet access and email to students is that student safety, security and sensibilities are not compromised. Despite this, it is not possible to absolutely guarantee that students will never access inappropriate sites or material while using District technology. It is understood that schools, staff, students and parents have a responsibility to provide the safest environment possible for students.

In order to support our students and build their understanding of digital citizenship and being safe online:

6.1 **Schools and school staff will:**

6.1.1 At a minimum, semi-annually review Internet and email safety procedures (see # 5) with all students.

6.1.2 Upon access to district-owned computers and BYOB computers, users will be presented with internet and email safety procedures;

6.1.3 Use only teacher-previewed and approved Internet sites with primary students;

6.1.4 Assist students in understanding that the Internet is an "open" environment and that some of the information available may be controversial, offensive, and/or inaccurate;

6.1.5 Teach to all of 6.2

6.2 **Students will:**

6.2.1 never give out such personal information as their name, age, home address, telephone number (s), photograph, their parents' or guardians' work address or telephone number or the name or location of the school over the Internet or through email;

6.2.2 never give out such personal information about other individuals over the Internet or through email;

6.2.3 immediately inform their parents, guardians, or a member of the District staff if they come across any information on the Internet or in an email that makes them feel uncomfortable;

6.2.4 not respond to any email or other message which makes them feel uncomfortable;

6.2.5 never agree to meet someone in person for whom they have 'met 'online without parental knowledge, permission, and supervision;

6.2.6 never agree to send or accept any item to or from a person whom they have "met' online without parental knowledge, permission, and supervision;

6.3 **Parents are encouraged to review the above with their child/ren several times each year or as appropriate for the child/children.**

7. Student Penalties for Non-compliance of any of the Network Procedures outlined in this Policy

Depending upon the severity of the infraction, the penalty for the breaking of any part of this Acceptable Use Policy will be based on a five-level scale of enforcement subject to the discretion of the school administration and/or District staff person responsible for technology.

1. verbal warning and/or other appropriate consequence
2. three-day suspension of network privileges
3. one-week suspension of network privileges
4. semester/year/permanent suspension of network privileges
5. legal action

8. Limitation of Liability:

The District makes no guarantee that the functions or the services provided by or through the District system will be error-free or without defects. The District will not be responsible for any damage you may suffer, including but not limited to, loss of data or interruption of service. The District is not responsible for the accuracy or quality of the information obtained through or stored on the system. The District will not be responsible for financial obligations arising through the unauthorized use of the system.

Link to Form:

APF 620-1 Staff Acceptable Use Form