DISTRICT TECHNOLOGY and NETWORKED INFORMATION

-POLICY-

The computing and telecommunication facilities and services provided by the Board of Education, School District No. 58 Nicola-Similkameen (herein after referred to as the Board) are intended for teaching, learning and administrative purposes. Access to district computing and telecommunication resources is a privilege, not a right. Every student and employee and other person having access to any district computing resources is required to use such resources in a legal, ethical, responsible and professional manner and to comply with Board policy governing the acceptable use of district technology and networked information under the following sub-sections of the Regulation:

602.61 District Technology and Networked Information - Acceptable Use
602.62 Electronic Communications Systems in Schools - Employee Acceptable Us
602.63 Electronic Communications Systems in Schools - Student Acceptable Use
602.64 Student Personal Technology Devices
602.65 Software Licensing
602.66 Webpage Content
602.67 Use of Personal Computers and Laptops at Schools and Other District Sites
602.68 District Filtering of Internet Access
602.69 Social Networking

602.61 - District Technology and Networked Information Acceptable Use

The computing and telecommunication facilities and services provided by the Board are intended for teaching, learning and administrative purposes. As such, district computing and telecommunication resources are used to enhance educational programs and to conduct district business. Access to district computing and telecommunication resources is a privilege, not a right.

Regulations:

1. This Policy and Regulations will govern all use of the SYSTEM, including student and employee use. When interacting on the Internet, users are expected to behave as they would in any other environment where they represent their school/employer as per school codes of conduct and/or professional codes of ethics.

2. Each student, employee and other person having access to any district computing resource is required to use such resources in a legal, ethical, responsible and professional manner.

3. The publication and posting of information on any district network or the World Wide Web is to be in accordance with ethical and legal standards and those derived directly from standards of common sense and courtesy that apply to the use of any public resource.

4. Students may be given access to the World Wide Web and may be given an individual E-mail account with the authorization of their parent/legal guardian. An Agreement signed by a parent/legal guardian will be required as a condition of access to the Web and provision of an individual E-mail account.

5. Each school is responsible for ensuring that all students who have access to electronic communications systems have an Agreement signed by the student and a parent/legal guardian. The Agreement can be signed once and filed for the student's remaining years in that school. Parents/Guardians will be able to sign a new form to alter current privileges at any time by contacting the school office.

6. Access to district computing and telecommunication resources may be withdrawn if employees or students do not comply with the Board policy governing the acceptable use of district technology and networked information and for other reasons as may be determined by the Superintendent.

7. The System administrator(s) has the right to suspend or terminate a user's access to and use of the System upon any breach of the Computer, Internet and BCeSIS Usage and Access Policy by the user. Prior to suspension or termination or as soon after as is practicable, the System administrator will inform the user of the suspected breach and give them an opportunity to present an explanation. The user may request a review hearing with the account authorizer (and/or other school district administrators) within seven (7) days of the suspension or termination if the user feels that the action was unjust. After the review, access may be restored if the System administrator and the school district personnel uphold the user's appeal.

602.62 – Electronic Communications Systems in Schools
Employee Acceptable Use

Employee use of district electronic communication systems must be in accordance with the following regulations. Access to district computing and telecommunication resources is a privilege, not a right.

Regulations:

1. Central system or network account holders are responsible for all usage of their accounts and, therefore, must keep their passwords confidential to protect themselves, their files and the district's files. Account holders must not distribute other users' identification (ID) and password or reveal other users' personal information.

2. District computer resources must not be used in a manner that may annoy or harass others. For example, distributing obscene, abusive, racist, threatening, unsolicited e-mail messages, or sexually/harassing messages or material.

3. Sensitive information must not be transmitted via or exposed to Internet access without taking appropriate measures to ensure data remains confidential.

4. All electronic communication, including e-mail, are the property of the Board and are subject to provisions under the Freedom of Information and Protection of Privacy Act.

5. Computer resources must not be used for personal use during instructional hours.

6. The use of district computer resources outside of instructional hours of work for personal reasons must be in accordance with these regulations and must not incur additional cost to the Board.

7. Non-acceptable usage of computer resources and networks include, but is not limited to, activities that:
    a. May lead to personal financial gain;
    b. Could be interpreted as gambling;
    c. Are used to conduct private business;
    d. Obscure the origin of any message under an assumed computer network address;
    e. Access illegal or offensive computer networks;
    f. Access or distribute unlicensed software or documentation;
    g. Initiate or distribute chain letters, advertising or unauthorized solicitations;

h. Access electronic systems or information inappropriately or without authorization;
i. Vandalize the system or system accounts;
j. Produce product and/or service advertisement or political lobbying;
k. Utilize network-intensive resources such as network games;
l. Violate or attempt to violate, the security of the system or attempt to subvert other systems;
m. Deliberately or recklessly expose systems to computer infections;
n. Contravene any laws or regulations.

8. Account holders must respect the rights of other users and consider the impact of their conduct on others.

9. Computer resource usage must be able to survive public scrutiny and/or disclosure. Users must avoid activities that might bring the Board into disrepute.

10. Computer resource use may be monitored without warning and inappropriate usage may be cause for cancellation of privileges and/or disciplinary action up to and including dismissal, or cancellation of contract.

11. Employees are responsible to ensure they have reviewed these regulations prior to making use of district computer resources.

602.63 – Electronic Communications Systems in Schools
Student Acceptable Use

Student use of electronic communication systems must be in accordance with the following regulations. Access to district computing and telecommunication resources is a privilege, not a right.

Regulations:

1. Students are responsible for their network accounts and all activity taking place in their allotted storage space and under their password. Passwords, therefore, must not be shared.

2. Students must not use another person's account.

3. School district resources must be used responsibly and not for any purpose except educational purposes.

4. Students must conduct themselves in a manner that respects the rights of others and should not include offensive or illegal behaviour.

5. Students using district electronic communications systems are expected to follow the same regulations both during and outside of school hours.

6. Parental written consent is required for students to access district electronic communications systems.

7. Teachers and Principals or designates are responsible for ensuring that all students who have access to electronic communications systems have read and signed a District Student Use Agreement (attached).

8. Teachers and Principals are responsible for taking appropriate disciplinary action when this policy is contravened.
    a. Illegal acts committed on or through district electronic communications systems must be reported to legal authorities.
    b. Illegal acts may include but not be restricted to hacking into systems or deleting files to which the student does not have access privileges, introducing viruses or downloading or copying copyrighted material.

602.64 – Student Personal Technology Devices

The use of all telecommunication and audio or video recording devices, including cellular phones, pagers/beepers and cameras, at schools and school-sponsored or school related activities on or off school property, is governed by the District AUP (Acceptable Use Policy) and their School Code of Conduct.

602.65 – Software Licensing

The Nicola-Similkameen School Board adheres to vendor software licensing agreements for the use of software in schools and district departments and acknowledges the licensing of software as copyrighted intellectual property.

Regulations:

1. Software placed on school computers must be done so in accordance with the vendor's licensing conditions. Schools and district departments must have a copy of the license for each corresponding software application.

2. Software purchased under an educational license must be used only on school and district computers or as defined by the licenses agreement.

3. Schools and district departments must keep a current record of all software licenses.

4. When software is purchased by the district, licensing information will be kept centrally in the district. When software is purchased by a school or department, it is expected that licensing information will be kept by the school or department.

5. When software is upgraded on the original license and placed into use, the original software must not be sold, given away or continued in use unless specifically stated in the licensing agreement.

6. Software no longer in use by schools or departments shall be disposed of through removal from all computers unless otherwise approved by the Superintendent or designate.

7. To ensure the consistent and legal disposition of licensed software all software disposal will be facilitated through the District Technology Coordinator.

8. Software licensing documentation must be held securely in the main office and made available to enforcement authorities upon request.

9. "Open Source" or software available under the General Public License (GPL) may be used freely as defined under the GPL.

10. All software must be pre-approved for installation by the Superintendent or designate.

602.66 – Website Content

The Nicola-Similkameen School Board encourages the use of the Internet/Intranet servers and the publishing of web pages to enhance the teaching and learning process and to foster communication within and outside the district. Subject to the following regulations, schools in the district have full control over the posting of web pages and may update or change school web pages at any time. The posting of web pages is a form of electronic publication, and is subject to all laws, including the Copyright Act and the Freedom of Information and Protection of Privacy Act. School web pages must also be designed to respond to concerns for student safety, privacy and security.

Regulations – Standard:

These regulations are intended to protect the privacy, safety and security of students and employees.

1. All web page information from district schools must reside on Nicola-Similkameen School Board servers. Departure from this procedure must be sought in writing from the Superintendent or designate prior to posting any school or department web page on third party provider servers.

2. Each principal must identify a person/s as the school web administrator who will be responsible for the school web pages.

3. The School District is required to comply with the provisions of FOIPPA. FOIPPA limits the use and disclosure of personal information to circumstances permitted by that Act.
   i. The FOIPPA authorizes the disclosure of employee contact information (such as name, work address, work telephone number, etc.).
   ii. However, student addresses, phone numbers and email addresses may not be disclosed on a School or Department web page.

4. Obtaining Consent and Authorization.
   Wherever possible, the District will attempt to obtain written authorization from a parent before posting any student personal information on School or Department Web pages. This provision does not apply to the posting of images taken at public events such as sporting activities or concerts. Parents will be asked to provide written authorization for the use of images taken other than in a public setting. The school or department should make efforts to obtain:

a. The district Media Consent Form for publishing activities. This should be signed when students initially register. Parents of students have the right to change this consent at any time.
b. Written consent for any specific publishing activity where a student name or photograph is used and that activity is not covered by the conditions set forth on the media consent form.

If required by FOIPPA, the District will attempt to obtain written authorization from an employee before posting any personal information concerning the employee on a District website.

5. Copyright - No content that breaches any copyright laws will be posted on a School or Department Web page.

6. Domain Names - All district materials for websites will reside under the school district domain name www.sd58.bc.ca. There will be no different domain names for district materials, except when approved by the Superintendent or designated committee.

7. The Board reserves the right to determine links posted on the district Web Page. Link postings may be monitored by the District Web Master.

602.67- Use of Personal Computers & Laptops at Schools and Other District Sites

The Board recognizes that staff and students may bring personal computers to their work location to help perform their duties (i.e. a teacher using a personal laptop to record marks, students using a personal device for Internet Access).

The Board accepts no responsibility for theft or damage that may occur to personal items brought to the school or the worksite.

The use of personal computers and laptops require the exercise of due diligence with respect to files containing work-related information, confidential information and student data.

To connect a personal computer and other network-enabled devices to the district network, the following conditions must be met:

a. A designated computer resource teacher or technician will be consulted to determine the network resources requested and the suitability of the equipment;
b. Staff will make prudent, work-related use of network resources;
c. Staff, students and special guests who bring personal computing equipment to district locations will be permitted to access the designated guest wireless network only. The designated guest wireless network allows users Internet Access and printing to a designated printer but not access to internal network services.
d. The Board assumes no obligation for the support of the personal equipment neither will it accept any liability for modifications made to the equipment as a result of establishing a connection;
e. The owner of the equipment will disconnect the equipment at the request of any supervisor.
f. The use of personal computers and laptops may result in the personal information of students (such as their names, student numbers, report cards or other information) or the personal information of others being stored on computers outside the district's computer network. The following safeguards, though not an exhaustive list, will assist in protecting privacy of personal information for both students and employees.

Employees must:

i. ensure that personal information stored on a computer or other data storage device is properly protected. Access to any personal information of a student or other person must be password protected, including when stored on any storage device, such as CD or USB drive. Any computer on which personal information relating to students or others related to the district must have effective Internet security measures such as licensed anti-virus software and firewalls.

ii. ensure that personal information of students and others is deleted from their personal computer, laptop or storage device as soon as possible and when the

data is no longer required for school district related purposes or when the teacher's employment ends.

iii. ensure that any school district related information located on a personal computer or laptop is collected, used or disclosed only for purposes and only in a manner permitted by the Freedom of Information and Protection of Privacy Act.

iv. be aware that any record of personal information obtained by the employee in the course of their duties may be subject to disclosure under the Freedom of Information and Protection of Privacy Act and may be considered to be in the possession and control of the School District, even if located on a personal computer or laptop.

602.68 – District Filtering of Internet Access

All requests for site filtering must be approved by the Superintendent or designate.
The District will filter Internet access if:

1. The site poses a danger to the integrity of our network.

2. The site allows for the circumvention of filtering software managed by PLNet.

3. The site places an inordinate amount of strain on network services because of bandwidth demand.

4. The site is specifically requested by the technology committee to provide for the unique protection of students at a particular grade level and the filtering is localized to the applicable schools.

5. The site is under temporary restriction as a school-based decision.

6. Other reasons as determined by the Superintendent of Schools.

602.69 – Social Networking

The Board of Education recognizes that part of learning is adapting to the changing methods of communication. It is important that teachers, students and parents engage, collaborate, learn and share in these digital environments.

Blogs, Wikis, Podcasts, Digital Images and Video and other Social Media Technologies

1. Personal Responsibility

    a) All users are personally responsible for the content/information they publish on-line.
    b) On-line behavior should reflect the same standards of honesty, respect and consideration used when meeting face-to-face.
    c) Posted information must identify that the information is representative of your views and opinions and not necessarily the views and opinions of the District.
    d) Social media is an extension of the classroom. What is inappropriate in the classroom should be deemed inappropriate on-line.
    e) Employees should ensure that posted content is consistent with the work performed for the District.
    f) Posting of confidential student information is prohibited.
    g) Employees are responsible for moderating all content published on all social media technologies.

2. Copyright and fair use

    a) All users must respect copyright and fair use guidelines.
    b) Plagiarism is an academic offence. Credit must be given where credit is due.

3. Profiles and Identity

    a) Last names, school names, addresses or phone numbers should not appear on blogs or wikis.
    b) Pictures and images must be appropriate and tasteful.

4. Personal Use of Social Media such as Facebook, Myspace and Twitter

    a) All users are personally responsible for all comments/information they publish on-line.
    b) On-line behavior should reflect the same standards of honesty, respect and consideration used when meeting face-to-face.

c) Posted comments should be within the bounds of professional discretion. Employees should act on the assumption that all postings are in the public domain.
d) Permission should be sought and granted prior to posting photographs and videos of others.

e) Photographs relating to alcohol or tobacco use may be deemed inappropriate.
f) Employees should refrain from posting any comment that could be deemed unprofessional.

5. Social Bookmarking

a) Sites that are bookmarked are in the public domain. The content of the bookmarked site should be within the bounds of professional discretion.