School District No. 63 (Saanich)

Policy Name: Use of Technology and Information Systems **No:** 3130

Preamble

The intent of this policy is to set expectations for ethical and appropriate use of the Internet and the district's network. This policy also indicates consequences for improper use.

The district maintains a network with an internet connection to support learning, educational and administrative communications of staff and students within and outside of the district. This network provides access to a variety of educational resources.

The district technology plan states that every student, administrator and staff member has appropriate and reasonable access to the online system within the school district and through the district system to external resources. This policy governs and guides that access.

Policy Statement

All users of school district networked systems will use those systems and will access resources in ways that are efficient, ethical and legal and consistent with the provisions of this policy, the District Technology Plan, the Provincial Learning Network (PLNet) agreement, and the Freedom of Information and Protection of Privacy Act (FOIPPA).

Statutory Reference: British Columbia's Freedom of Information and Protection of Privacy Act (FOIPPA)

Contractual Reference: Provincial Learning Network (PLNet) Agreement

Policy Reference: 3100 – Selection of Learning Resources
3120 – Challenge of Learning Resources
District Technology Plan

Date of Initial Board Approval: July 1982 **Amendments:** June 2014
November 1989
May 1990
June 2008
April 2011

School District No. 63 (Saanich)

Policy Name: Use of Technology and Information Systems **No:** 3130

Guiding Principles

1. All access by students, staff and volunteers, including parents, to district-mediated online communications is governed by this policy.

2. Electronic information will only be stored and retrieved as necessary and in ways that are consistent with the FOIPPA and the provisions of this policy.

3. Staff and student access to online information and communication is a critical part of education. Electronic communications extend learning opportunities and increase awareness of and access to global resources and perspectives.

4. An inclusive learning environment requires equitable access to the internet.

5. Student access to online resources should be developed in a collaborative learning environment in supervised contexts and be accompanied by instruction and high expectations about safety, ethics, etiquette and appropriateness of material.

6. The choosing and recommending of online sites and resources by teachers is governed by the criteria for selection listed in Policy 3100 - Selection of Learning Resources and is subject to the challenge process outline in Policy 3120 - Challenge of Learning Resources.

7. Parents are required to give consent before students are permitted to participate in teacher driven use of web-based tools where personal information may be used. Where consent is not given an alternative must be provided.

8. Students are expected to abide by school Code of Conduct when using district communication networks.

9. Students and parents are responsible for online behaviour outside the school setting. However, sometimes the actions of students have impacts on the school community and may need to be addressed by administration, the school district, and/or law enforcement as outlined in Policy 6110.

10. Consequences for inappropriate uses are outlined in the administrative procedures and will be consistent with other disciplinary procedures within the district.

Guiding Principles (cont'd)

11. The Board supports and endorses the use of technologies which are environmentally friendly that minimize waste in creation and disposal and that minimize potential health concern.

12. The Board supports the purchase of energy efficient and long-life equipment and technologies as a means of reducing overall energy costs.

13. Although the district technology plan is predicated on hard-wired access to the internet through thin client technologies, the Board recognizes that there are circumstances where wireless access to the internet is desirable. Wireless access will be made available in accordance with the provisions of Administrative Procedure 19 as needed and in compliance with the safety standards established by Health Canada and the World Health Organization. Those safety standards will be reviewed from time to time by the Superintendent of Schools. Commercial-grade managed wireless access points will be provided in adult work spaces including the school board office, physical plant, education centre, school staff rooms and staff work areas, and in student environments in accordance with Administrative Procedure 19. It is understood that where WiFi access is intentionally limited to certain areas of schools there will be some degree of radio-frequency signal evident throughout the school diminishing in intensity as a function of (the square of) the distance from the wireless access point.

School District No. 63 (Saanich)

Policy Name: Use of Technology and Information Systems **No:** 3130

Administrative Procedures

1. Purposes
   The district network and internet connectivity will be managed in a way that supports and enhances educational opportunities for students and staff. The district network will be maintained in a way that facilitates communication among staff, students and the community, and provides access to appropriate online resources.

2. District Rights
   The district has the right to restrict or terminate access to and through its network at any time for any reason. The district further has the right to monitor any network activity in order to maintain both the operation and appropriate use of the information network.

3. Privacy
   The district will store electronic information only as necessary and in ways that are consistent with the FOIPPA and the provisions of this policy. The district will routinely monitor internet use.

4. Confidential Information
   Users are expected to exercise due diligence with content containing school-related and confidential information.

5. Appropriate use of Internet Access
   The District network is a shared resource and access to the internet is limited. Users of the district network are part of a community and are expected to use the resource in a way which does not negatively interfere with the needs of others. Streaming videos and other high-bandwidth usage of the district network for non-educational purposes is not appropriate.

6. Storage Capacity
   Users are expected to delete non-essential email or other material that take up excessive space. Disk space storage and email limits may be imposed on both staff and students.

7. District staff email
   a) The district assigned email account shall be an official means of communication for all staff. District-owned email systems are no different from district-owned telephone systems, bulletin boards, copiers or other capital assets and are to be treated in the same manner. Users are responsible for all information exchanged via their district assigned email account.

Administrative Procedures (cont'd)

i) The account and the contents of the account are governed by administrative procedures.
ii) The district offers this service on an as-is basis. The district information technology department does not offer any implicit or explicit guarantees of service.

b) It is the account holder's responsibility to create a secure alphanumeric password in accordance with District requirements.

c) The IT department will create new email accounts for new staff members upon notification from the Human Resources department and will retain those accounts until retirement, resignation or termination of the staff member.

e) When a staff member leaves the district by retirement, resignation or termination, the email account will be deleted. The account holder is expected to clear the account of personal correspondence before leaving. Human Resources is responsible for notifying the IT Department as to the deletion date.

f) The district will make reasonable efforts to maintain the integrity and effective operation of its electronic mail systems, but users are advised that those systems should not be regarded as a secure medium for the communication of sensitive or confidential information. The nature and technology of electronic communication does not allow the district to assure the privacy of an individual's use of the district's electronic mail resources or the confidentiality of particular messages that may be created, transmitted, received or stored thereby.

8. Use of Personal and Wireless Devices
The district recognizes that staff and students may bring their own computers to school/work to help perform their duties. Personal devices may only attach to the internet (PLNET) via public wireless. Personal devices will not be given access to the wired network.

a) Up-to-date virus protection software must be licensed and installed for the computer.
b) The computer must be running an operating system that allows for appropriate network security to be applied.
c) Use of personally owned computers will only be for appropriate work and learning purposes.

Administrative Procedures (cont'd)

d) The district assumes no obligation for the support of the personal equipment; nor 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 or Information Technology staff member.
f) The Board accepts no responsibility for theft or damage that may occur to personal items brought to the school or the worksite.

9. Software Licensing

The district adheres to vendor software licensing agreements for the use of software in schools and district departments and acknowledges the licensing of software as copyright intellectual property.

a) Open Source or software available under the General Public License (GPL) may be used freely as defined under the GPL. Open Source software is to be considered as the preferred alternative to commercial software wherever possible.
b) 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.
c) Software purchased under an educational license must be used only on school and district computers or as defined by the license agreement.
d) Schools and district departments must keep a current record of all software licenses.
e) Where software is purchased by the district for distribution to schools/departments, licensing information will be kept centrally in the district.
f) Where 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.
g) Software no longer in use by schools or departments should be removed from all computers.
h) Removal may include destruction, selling or giving away the original copy and documentation provided this does not contravene the original licensing agreement.
i) Software licensing documentation must be held securely in the main office and made available to enforcement authorities upon request.

Administrative Procedures (cont'd)

10. Online Publishing and Communication
It is the expectation that schools, departments and programs will use district provided online communication tools hosted on district servers.

Departure from this procedure at school level must be sought in writing from the Superintendent or designate prior to posting any school web page on third party provider servers.

Departure from this procedure by a department or program must be sought in writing from the school administrator prior to posting any department or program web page on third party provider servers.

Schools, departments and programs interested in using third party online communication tools, used in conjunction with district provided tools, must contact the IT Director or designate to ensure that district-wide practices and procedures are followed. i.e., naming conventions/theming.

a) Each principal or designate must identify the school's site manager(s), who will be responsible for managing the content of school web pages.

ii) Each principal or designate must identify the person(s) who will be responsible for managing/publishing content on third party online communication tools.

All graphic, photographic, video, audio and multimedia content appearing on a district or school webpage used for business purposes must be original source material. Materials owned through other sources or copyright materials must be accompanied by written authorization from the owner or copyright holder before publication or posting on district web servers or other internet sites.

All graphic, photographic, video, audio and multimedia content appearing on a district or school webpage used for educational purposes that are not original source material must be attributed and authorship identified in accordance with the fair dealing rules in Canadian copyright law.

Each school main website must contain prominent link pointing back to the district webpage.

b) All published materials on district servers become the property of the district. The district retains full copyright on all posted web content. All original student work posted to the district or other websites is the property of that student.

Administrative Procedures (cont'd)

11. Student Personal Information

    a) Schools and Districts are authorized to collect, use, and share student personal information that is directly related to and necessary for their educational functions. For other school or education-related purposes, parental consent is required.

    b) Saanich School District will seek consent to collect, keep, use and share photographs, videos, work, and names of students on the school or district website(s) and other publications for education related purposes, such as recognizing and encouraging student achievement, building the school community, and informing others about school and district programs and activities. This may include publications such as newsletters, brochures, and reports, social media sites, and online video (e.g., YouTube).

12. Web-Based Tools

    a) The district recommends teachers utilize district provided and hosted web-based applications such as Moodle and Elgg.

    b) Schools and teachers may also request that students use other web-based tools, not hosted by the school district, to create and share their learning. Using these tools, students may:

        - Create accounts using personal information (i.e., email address)
        - Publish/present student pictures/video/audio, with names and personal information
        - Create/communicate/collaborate/network in online communities

    c) When web-based tools are used parent consent is required if any of the above (b) occur. Teachers will obtain parent consent through the use of the web-based tools consent form and a cover letter outlining (b), as well as, the educational purpose for using the web-based application.

    d) Terms of use should be followed when using online tools.

    e) Internet safety, digital citizenship and literacy will be taught explicitly and revisited regularly. Teachers and students will be learning alongside children in Saanich schools, our school district, and around the world. As a general safe practice, when interacting with any web-based service, students should take care and avoid posting personal information that could be used to identify themselves

Administrative Procedures (cont'd)

or other people. Student's personal information may be accessible by others with the creation of an account on a web-based tool, through the content created and published by students and the actions of others.

13. Outside Media
Media (including radio, television, newspapers, and other print and online media) are sometimes permitted or invited to come to the school or to school activities and allowed to take photos or video or conduct interviews with students, for the purposes of promoting public understanding of school programs, building public support for public education, and encouraging student achievement.

School and district staff cannot control news media access, photos/videos taken by the media or others in public locations (such as field trips or off school grounds) or at school events open to the public, such as, sports events, student performances, school board meetings, etc.

Parent consent is required when student personal information is captured by outside media. If parents do not want their student to be involved in such activities, parents need to: tell their child to avoid these situations, tell their child's teacher of your wishes.

14. Ethical Use
Any use of email or access to network or internet resources by students or staff which are contrary to the purposes of the network or which violate or endanger personal safety, legality, system security, or privacy are prohibited. These practices include but are not limited to:
- use for political or commercial gain
- use that is not consistent with the educational purposes of the network;
- use of profanity or inappropriate language;
- use that disrupts the educational goals of the district;
- use of a district account by unauthorized users;
- access of material that has been deemed inappropriate for school use including pornography;
- use that violates copyrights or license agreements;
- use that intentionally disrupts network traffic or degrades equipment or network performance;
- illegal activities including harassment;
- use that invades the privacy of individuals;

Administrative Procedures (cont'd)

- possession of data in any form which might be considered a violation of these practices

15. Inappropriate Materials
Staff and students will be allowed to use this network to access the internet understanding that some material that is available through the internet is inaccurate or biased and must be used with caution. Some material is contrary to prevailing community standards and is inappropriate for classroom use. Access of inappropriate material is not permitted through this network. While the district will attempt to reduce the accessibility of objectionable material, the internet is designed to make all materials within it available through search and retrieval tools. While the district and PLNet include content filtering, the primary tool in preventing access of inappropriate materials is the development of an ethical user.

Students and parents need to know that it is possible for students to encounter inappropriate material during legitimate research. If a student inadvertently encounters inappropriate material the website should be left immediately. Students and staff need to constantly evaluate and filter information and resources in the internet environment.

16. Code of Conduct for district network
The following items must be included in Code of Conduct of each school:
    - Students will engage in appropriate curricular behaviour when using the district network.
    - Students will only publish their own personal information if related to curricular activities and parent/guardian consent is given.
    - Students will not publish other people's personal information. For example, name, location, phone number, images, video, work, username, or other personal information.

17. Consequences of violations include but are not limited to:
    - suspension or revocation of network privileges;
    - suspension or revocation of computer access;
    - school suspension;
    - disciplinary action of an employee under the appropriate collective agreement or contract of employment;
    - legal action and prosecution by the authorities.

Administrative Procedures (cont'd)

18. Forms
Consent forms relating to student's personal information and use of web-based tools are available for distribution and school administrators should ensure that the consent forms are completed by students and/or parents at the appropriate time during the school year. Forms are located in the Zimbra briefcase and The Hub: http://hub.sd63.bc.ca

19. Although the district technology plan is predicated on hard-wired access to the internet through thin client technologies, the Board recognizes that there are circumstances where wireless access to the internet is desirable. Wireless (WiFi) installations will be managed as follows:

    a. There will be no WiFi installations in elementary schools except as authorized by the Superintendent of Schools in response to submissions from schools that are:
        - based on thorough consultation within the school community;
        - in keeping with Guiding Principles 13;
        - clear in the assertion that installation of WiFi is required for student learning and support;
        - designed to minimize locations and time of use of WiFi
    b. In middle and secondary schools, managed WiFi environments may be installed in adult workplaces including staff rooms and offices as necessary.
    c. Middle schools will have up to 25% coverage of student areas (with the understanding being that there will be spillover of the signal as described in Guiding Principles 12), with the locations to be determined in accordance with educational needs as described in IEPs and overall educational needs for the school as determined with staff and the Parent Advisory Council.
    d. Secondary schools will have school-wide WiFi coverage.
    e. The Information Technology Department will be responsible for all WiFi installations and will ensure that all wireless access points are managed, commercial grade and as localized as possible.

20. School administrators will review this policy with all staff at the beginning of each school year and will make paper copies available to parents upon request. District administrators and supervisors will ensure that employees not assigned to schools review this policy on a regular basis.

Administrative Procedures (cont'd)

21. The District is committed to moving to a common and consistent IT platform in order to more effectively use and manage resources. To ensure that devices are compatible with District infrastructure, that they can be effectively managed by IT staff, and that they are of a suitable commercial grade, schools must consult with the District Information Technology department to discuss any potential IT purchases. Examples of these devices include desktop and laptop computers, printers, photocopiers, tablets, document cameras, and LCD projectors. If the devices are not compatible with district systems, or cannot be effectively managed, the devices may not be purchased. To support the management of portable devices, the district will use a mobile management system. The initial licence per device will be purchased by the district and the school will be responsible for any additional monthly costs.