Personal Electronic Device Policy

This policy applies to all electronic devices whether owned or leased by the school or the user. This policy also applies to all users of PEDs and school-based technology including, but not limited to, students, staff, parents, and volunteers.

Procedure

1. The school Principal will ensure that students and staff are made aware of the benefits and risks associated with the use of PEDs and school-based technology and are made aware of this policy.

2. All schools must include a student PED and school-based technology policy statement accompanied by the general definitions of a PED and school-based technology in their student/parent handbook and website link.

3. All schools must develop and enforce local policies and procedures for the use of PEDs and school-based technology wherein students and parents are informed of the restrictions and conditions of use.

4. All schools must teach students and staff members the appropriate and responsible use of PEDs and school-based technology.

5. All schools must develop rules and an Acceptable Use Agreement that applies to PEDs and school-based technology.

6. Individuals are expected to abide by the school's conditions with respect to the permitted use of PEDs and school-based technology as outlined below.

7. There is a diminished expectation of privacy on any PED brought into the school. Teachers and school administrators are responsible for providing a safe environment and maintaining order and discipline in the school. This responsibility may, in certain circumstances, require them to search for and/or temporarily confiscate a student's PED where they have a reasonable suspicion that a student is in breach of school policy.

8. Any individual who willfully breaches this policy or otherwise engages in inappropriate use of personal PEDs on school property, a school-issued PED or school-based technology generally, may be subject to sanctions including the restriction of their ability to access and use PEDs or school-based technology and, in the case of students or employees, may be subject to disciplinary action. General School Administration Personal Electronic Devices and School-based Technology Policy 430.

9. Violations of this policy will be reported to the appropriate law enforcement authorities where required and may also be subject to criminal investigations and/or criminal charges.

Permitted Uses of PEDs

The following conditions apply with respect to the use of PEDs on school premises or during school sanctioned activities, as well as the use of school-issued PEDs:

1. The school may integrate PEDs into the learning and teaching environment and, if so, must have an educational plan for such use.

2. The school Principal (or designate) may authorize the use of a PED on the school premises (or during school-sanctioned activities) for a specific designated purpose. The school Principal (or designate) may provide specific instructions pertaining to a limited acceptable use of PEDs during extraordinary circumstances including emergency conditions (evacuation, lockdown, heightened risk, etc.).

A. Rules for the use of both PEDs and School-based Technology:

1. All individuals are expected to use PEDs and school-based technology in a courteous, respectful, and otherwise appropriate manner consistent with school and CISVA policies, and the guidelines and expectations outlined in the school code of conduct.

2. The electronic transmission or posting of digital content relating to staff or students, either through the use of school-issued PEDs, school-based technology or personal PEDs while on school property, is prohibited without the express permission of the person or persons involved. In cases where a student is below the age of 19, the consent of the parent/guardian is required.

3. Prohibited uses of PEDs and school-based technology include, but are not limited to, the use of PEDs or school-based technology that:

a. compromises the academic integrity of the school or an individual within the school.
b. interferes with or disrupts the academic day or the teaching/learning environment.
c. violates a person's reasonable expectation of privacy (including, but not limited to, taking, distributing, or posting photos of other persons without their consent).
d. compromises personal and/or school safety (including, but not limited to, cyber bullying, and posting information about themselves or others that may put them at risk).
e. facilitates illegal and/or unethical activities, including but not limited to:
    i. transmitting materials in violation of Canadian laws;
    ii. receiving, viewing, duplicating, storing, or transmitting pornographic materials;
    iii. transmitting or posting threatening, abusive, or obscene messages or materials;
    iv. duplicating, storing, or transmitting any material that contravenes the

Copyright Act;

v. installing or reproducing unauthorized or unlicensed software;

vi. sending, linking to, or otherwise making available material likely to be offensive, objectionable, or pertaining to criminal skills or activities with a criminal application and intent.

vii. utilizing applications to facilitate the downloading or exchange of music, movies, games or other materials in contravention of the Copyright Act;

viii. forging any document or message; obscuring the origin of any message, transmission, or file;

ix. using programs that harass users, prevent access, investigate, or infiltrate computer systems /or software components;

x. promoting commercial uses or product advertising; and

xi. participating in online gambling sites.

4. The RCAV, CISVA and school will not be held responsible for any damage that may occur to a PED as a result of connecting to any school-based technology or any electrical power source.

5. The parents and/or guardians of any student bringing PEDs to school are responsible for and will reimburse the school for any damage that their child may cause through the use of school-based technology with his/her PED.

B. Rules for the Use of School-based Technology:

1. Users are responsible for their own individual account and must take all reasonable precautions to prevent others from being able to use their account. Users shall change their password, seeking assistance from a staff member if necessary, if they believe that others may know of their password.

2. Users will not attempt to gain unauthorized access or go beyond their authorized access by entering another person's account password, accessing another person's files, or 'hacking' into any unauthorized accounts.

3. School-owned or leased electronic devices are not permitted to be taken out of the school building unless the internet capabilities of the device are disabled or appropriately filtered.

4. Users shall not intentionally disrupt, or attempt to disrupt, school-based technology or any other computer system, or destroy data by spreading computer viruses or by any other means.

5. Users shall not disable or otherwise interfere with or modify the virus scanning, security or network settings installed in any school-based technology that is used.

6. Users shall immediately notify a teacher upon discovery of a possible security problem.

7. Users shall not download or attempt to run or store any app and/or program file not authorized by the school.

8. Students shall not attempt to install any software applications. All software is to be installed and configured by school staff.

9. Users shall not take actions that place an excessive load on the School's network as to restrict or inhibit other Users from using school-based technology or impacting the efficiency of the network.

10. Each school must maintain an active filter system and/or other technologies that attempt to block a User's access to Internet material that is obscene, pornographic, inappropriate, (including non-age appropriate), or potentially harmful to minors, is not related to school business, or otherwise violates any school rules.

11. Users shall not make any intentional (with knowledge that access to such materials they are seeking are blocked) attempt to bypass the school's filters or access any blocked materials.

12. The school Principal, or his or her delegate, has the right to monitor any network activity that utilizes school-based technology in order to maintain its operation and appropriate function.

Definitions

Account means the User ID and Password assigned to an individual for access to a school computer and/or network resource, which may include a third party service provider utilized by the school for educational purposes.

Filter means a specific technology that blocks or filters access to specific Internet resources, including those that are:
1. Illegal;
2. Obscene;
3. Harmful to Minors; or
4. Unrelated to the school's educational mission.

Personal Electronic Devices (PEDs) are wireless and/or portable electronic handheld equipment that include, but are not limited to, existing and emerging Mobile Communication Systems and Smart Technologies and any other convergent communication technologies that do any number of functions. PEDs also include any current or emerging wireless handheld technologies or portable IT systems that can be used for the purpose of communication, entertainment, data management, word processing, wireless internet access, image capture/recording, sound recording and information transmitting/receiving/storing, etc. PEDs include, but are not limited to, laptops, phones, tablet computers, wearable technology such as glasses or watches, and cameras.

School-based Technology: means all CISVA school-based networks, including, but not limited to, school servers, school computers, school software, school printers, online services provided by the school, and networks (wired or wireless), which connect all of the above to the Internet.

User means any individual who uses, logs in, attempts to use, or attempts to log into School-Based Technology (by direct connection or across one or more wired or wireless networks) or who attempts to connect to or traverse school-based technology or who uses hardware or software belonging to a school.

The term User includes any CISVA staff, students, parents and volunteers who attempt to use school-based technology.

SFDS Staff Acceptable Technology Use Policy

The use of PEDs and school-based technology should in no way interfere with the safety, security and privacy of students and/or staff.

In addition, the use of PEDs and school-based technology should not interfere in any way with student learning and school operations.

PEDs include, but are not limited to, laptops, phones, tablet computers, wearable technology such as glasses or watches, and cameras.

I understand that I am expected to use PEDs and school-based technology in a courteous, respectful, and otherwise appropriate manner consistent with school and CISVA policies, and the guidelines and expectations outlined in the school code of conduct.

I understand that the electronic transmission or posting of digital content relating to staff or students, either through the use of school-issued PEDs, school-based technology or personal PEDs while on school property, is prohibited without the express permission of the person or persons involved. In cases where a student is below the age of 19, the consent of the parent/guardian is required.

I understand that the RCAV, CISVA and SFdS will not be held responsible for any damage that may occur to a PED as a result of connecting to any school-based technology or any electrical power source.

Prohibited uses of PEDs and school-based technology include, but are not limited to, the use of PEDs or school-based technology that:

a. compromises the academic integrity of the school or an individual within the school.

b. interferes with or disrupts the academic day or the teaching/learning environment.
c. violates a person's reasonable expectation of privacy (including, but not limited to, taking, distributing, or posting photos of other persons without their consent).
d. compromises personal and/or school safety (including, but not limited to, cyber bullying, and posting information about themselves or others that may put them at risk).
e. facilitates illegal and/or unethical activities, including but not limited to:
    i. transmitting materials in violation of Canadian laws;
    ii. receiving, viewing, duplicating, storing, or transmitting pornographic materials;
    iii. transmitting or posting threatening, abusive, or obscene messages or materials;
    iv. duplicating, storing, or transmitting any material that contravenes the Copyright Act;
    v. installing or reproducing unauthorized or unlicensed software;
    vi. sending, linking to, or otherwise making available material likely to be offensive, objectionable, or pertaining to criminal skills or activities with a criminal application and intent.
    vii. utilizing applications to facilitate the downloading or exchange of music, movies, games or other materials in contravention of the Copyright Act;
    viii. forging any document or message; obscuring the origin of any message, transmission, or file;
    ix. using programs that harass users, prevent access, investigate, or infiltrate computer systems /or software components;
    x. promoting commercial uses or product advertising; and
    xi. participating in online gambling sites.