SCHOOL DISTRICT NO. 64

"Inspire learners, Integrate sustainability, Involve community"

PROCEDURE 220
Information Systems: Acceptable Use and Protection of Privacy

Section: Learning and Working Environment
Dates of Revisions:
Date of Adoption and
Resolution Number: June 13, 2018- 76/18

---

1. Access to information systems, including Internet resources is voluntary and a privilege, not a right.

2. Access is available only so long as the user complies with Board policies, administrative procedures and local, provincial and federal laws.

3. Users will conduct themselves in a courteous, ethical, and responsible manner while using these systems. All Board policies and administrative procedures, including those on harassment, equity, and proper conduct of employees and students apply to the use of information systems.

4. Inappropriate or prohibited use may lead to suspension or termination of user privileges, legal prosecution or disciplinary action appropriate under any applicable laws, policies, regulations, collective agreements or contracts.

5. Although the District take reasonable steps to screen or limit access to offensive/inappropriate material while preserving the educational value of the system, the dynamic nature of online information services makes total regulation and control impossible. The District adheres to Provincial Learning Network monitoring and reporting protocols.

6. Students must be aware that:

    a. Activities on information systems are not private, and may be monitored or reviewed at any time. Nothing is to be done on an information system that the student does not want other students, school staff, or the District staff to see.

    b. It is rare but possible to accidentally access inappropriate materials. Students are to immediately report such events to District staff and then return to appropriate materials.

7. Because there is a wide range of material available on the Internet, some of which is offensive and in conflict with the values of some students, parents or guardians

a. parents/guardians are advised to caution their children regarding material that they think would be inappropriate for their children to access.

b. the District fully expects that students will follow their parents/guardians' instructions in this matter.

8. Student Access to Information Systems

a. All students may have access to District information systems through their classroom, library, or school computer lab where such access exists or from home.

b. Students must accept responsibility for learning, and using, the systems appropriately for educational or research purposes. Failure by a student to comply with this administrative procedure, and any rules and regulations regarding use of the electronic system may result in suspension or revocation of access privileges and disciplinary action.

c. Students access will be appropriate to their educational needs and developmental levels.

d. Authorization for District email access may be granted to a student, only when the student agrees to be bound by this administrative procedure and any rules and regulations respecting use of the system that are made by the District from time to time.

e. Parent consent is required. If parents do not want their children to have access to the district Network or Internet, they must inform the child's school in writing each year.

f. The purpose of student access to the information systems is student learning and education, including, but not limited to:
    i. training in the use of computer systems;
    ii. accessing a wide range of materials with educational value to the student; and
    iii. communicating with others around the District and the world to enhance the student's education.

9. Staff Access to Information Systems

a. Staff are encouraged to use the electronic system in the conduct of their work, and to find innovative and effective ways to enhance education and District business.

b. Staff may use the information systems during breaks and before and after normal business hours for personal communications, research, and education purposes that do not interfere with District educational and business use.

c. Such access must be appropriate and legal and is subject to all parts of this administrative procedure.

d. Personal use is understood to be at a lower priority than educational or District business use, and subject to interruption without notice.

e. Staff are required to comply with this administrative procedure and any rules and regulations regarding use of the electronic system that are made by the District. Failure to do so may result in suspension or revocation of access privileges and disciplinary action subject to the collective agreements.

f. Any staff using a District information system, including email, network access and/or Internet access, must agree to abide by this administrative procedure and complete an Acceptable Use Agreement form (Form 220-1) prior to use.

10. Access to Information Systems by Guests and Others

a. Guest access to District information systems may be extended to trustees, parent members of Parent Advisory Councils, members of other school districts, or other members of the education community.

b. Guests are required to comply with this administrative procedure and any rules, procedures, and regulations regarding use of the electronic system that are made by the District. Failure to do so may result in suspension or revocation of access privileges.

c. Any guest using a District information system, including email, network access and/or Internet access, must agree to abide by this administrative procedure and complete Acceptable Use Agreement (Form 220-1), prior to use.

11. Security

a. The use of student information within information system tools is subject to the Freedom of Information and Protection of Privacy Act (FIPPA), as outlined in Policy 131.

b. Users are responsible for their access to information systems and are to take all reasonable precautions to prevent others from being able to use it. For example, users are not to write any password on a post-it note and leaving it in view or save a password in a password list.

c. Under no conditions are users to provide their password to another person other than a system administrator.

d. Users must log off their workstations when not in use to avoid unauthorized access.

e. Users will immediately notify a teacher or the system administrator if they have identified a possible security problem. However, they are not to go looking for security problems, as this may be construed as an illegal attempt to gain access.

f. Users will not make use of anti-security programs such as, but not limited to, keyboard loggers, password crackers, or unauthorized remote access software.

g. If student users mistakenly breach security or find a virus, they are to immediately tell their teacher or another District employee or disclose this access in the manner specified by the school. If staff users mistakenly breach security or find a virus, they are to immediately tell their supervisor or disclose this access in the manner specified by the school or work site. This may protect them against a claim that they have intentionally violated this administrative procedure.

12. Personal Safety of Users

a. District staff will not post student personal contact information without the consent of the student's parent/guardian or of the student if of legal age. This includes a student's address, telephone number, school address, work address, or any information that clearly identifies an individual student.

b. Students' first names and initials may be used in school on-line newsletters.

c. Students and parents need to be aware of certain dangers about Internet use in general.

d. Students are not to post personal contact information about themselves or other people. Personal contact information includes but is not limited to: address, telephone, school address, work address.

e. Students are not to agree to meet with a contact they have only met online.

f. Students and parents need to be aware that harassment and bullying occurs on the Internet and that students are to report any incidents to their parents.

g. Parents are to report such activity to the appropriate authorities.

h. Students will promptly disclose to their teacher or other District employees any messages users receive at school that are inappropriate or make them feel uncomfortable.

i. Student and staff account information, as well as any documents uploaded onto on-line collaboration and productivity tools platforms will be
    i. stored on secure servers located beyond Canada, and may be subject to the laws of foreign jurisdictions.
    ii. subject to access by the tool proprietor's employees only when a district administrator grants explicit access for troubleshooting purposes.

13. Privacy and Confidentiality

a. Users will not
    i. repost, copy, forward, or otherwise distribute a message that was sent to them marked "private" or identified in the content as "confidential", without permission of the person who sent them the message;
    ii. repost, copy, forward, or otherwise distribute any information from a District confidential database, including, but not limited to, student,

(example: Individual Education Plans), financial, payroll, or personnel, to unauthorized persons.

iii. post, copy, forward, or otherwise distribute private information about another person.

b. Use of district information systems including the Internet, by any individual, may be monitored or reviewed by District system administrator(s) and/or Provincial Learning Network system administrators without prior notice

c. The contents of computer hard drives and other storage devices owned, operated or maintained by the District may be accessed by the system administrator(s) without prior notice.

d. The system administrator(s) may block messages or remove files that are unacceptable and/or in violation of Board policies or administrative procedures.

e. The system administrator(s) will not intentionally inspect the contents of users' email, or disclose the contents to anyone other than the sender, or intended recipient, without the consent of the sender or intended recipient, unless required to do so by law or the policies of the District, or to investigate complaints regarding electronic files which are alleged to contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material.

f. The District will cooperate fully with any participating District, local, provincial, or federal officials in any investigation concerning or relating to any electronic files transmitted on District information systems.

g. In cases where files have been accessed, efforts will be made to inform users within a reasonable time period of any action that is taken.

h. Parents/guardians have the right at any time to request to see the contents of their child's District email files where legally applicable.

14. Inappropriate Language and Behaviour

a. Restrictions against inappropriate language apply to public messages, private messages, and material posted on Web pages.

b. Users will not

i. use language or imagery which violates district policy because is obscene, profane, lewd, vulgar, rude, racist, inflammatory, discriminating, threatening or disrespectful.

ii. post information that could cause damage or pose a danger of disruption to the District.

iii. engage in personal attacks, including but not limited to prejudicial or discriminatory statements.

iv. harass other persons.

v. knowingly or recklessly post false or defamatory information about a person or organization.

c. If student users mistakenly post information that might be considered inappropriate, they are to immediately tell their teacher or other District employee. If staff mistakenly post information that might be considered inappropriate, they are to immediately tell their supervisor or system administrator. This may protect users against a claim that they have intentionally violated this administrative procedure.

15. Inappropriate Access to Material

a. Users will not deliberately access material that:
   i. Is profane or obscene such as, but not limited to, pornography;
   ii. Advocates illegal acts; or
   iii. Advocates violence or discrimination towards other people such as, but not limited to, hate literature.

b. If student users mistakenly access inappropriate information, they are to immediately inform their teacher or other District employee. If staff users mistakenly access inappropriate information, they are to immediately tell their supervisor. This may protect users against a claim that they have intentionally violated this administrative procedure.

16. Plagiarism and Copyright Infringement

a. Users will
   i. not plagiarize the works of others, found on the Internet or elsewhere. (Plagiarism is taking the ideas or writings of others and presenting them as their own.)
   ii. respect the rights of copyright owners. Copyright infringement occurs when users inappropriately reproduce a work that is protected by a copyright.

b. If a work contains language that specifies appropriate use of that work, users are to follow the expressed requirements.

c. If it is not clear whether or not a work can be used, users are to request permission from the copyright owner.

d. If copyright cannot be explicitly determined, users are to presume that it exists.

17. Illegal Activities

a. Users will not attempt to gain unauthorized access to any District computer system or to any other computer system through the District or go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of "browsing".

b. Users will not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. These actions are illegal.

c. Users will not use the access provided to engage in any other illegal act, such as, but not limited to, arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, or threatening the safety of a person.

d. If students mistakenly commit an act that might be considered illegal, they are to immediately tell their teacher or other District employee; or disclose this access in the manner specified by the school. If staff mistakenly commits an act that might be considered illegal, they are to immediately tell their supervisor or disclose this access in the manner specified by the school. This may protect them against a claim that they have intentionally violated this administrative procedure.

18. Respecting Resource Limits

a. The primary use of District information systems is for educational, career and professional development and the business activities related to operation of the District. Reasonable limits may be imposed in order to safeguard the efficient operation of the system and to respect the rights of all users.

b. Limited personal use of District resources, subject to all of the foregoing regulations, will be permitted providing that there are system resources available. Users may be required, from time to time, to refrain from personal use of resources due to educational and/or operational needs.

c. Users will not
    i. download large files unless absolutely necessary. If necessary, they will download the file at a time when the system is not being heavily used such as after class or business hours and immediately remove the file from the system computer to removable media. Users may be asked to terminate a large download if such activity impairs the efficient operation of the system or an educational activity.
    ii. post chain letters.
    iii. download, install and/or use any unauthorized peer-to-peer file sharing software.
    iv. download, install and/or use any unauthorized gaming software.

d. Users will check their email frequently, delete unwanted messages promptly, and stay within their account quota as assigned by their system administrator.

e. To safeguard the resources of a network system the system administrator may set a disk quota that users will have to adhere to.

19. Software Installation

a. Users will install software on a classroom computer or computer system assigned for their use only where they are permitted to do so. Such software must be legally licensed.

b. Users will not install software that they have purchased for home use on a District system, unless they remove the software from their home computer and donate the license, media and documentation to the District.

c. Users will not install software that does not have a legal license on a District system.

d. Users will not utilize district licensed software on personal owned systems. The exception is Microsoft Home Use Program while employed. There are terms and conditions and a cost with this application – please reference the most up to date guidelines from Microsoft.

20. System Administration

a. While circumstances might dictate that a system administrator must investigate or remove files or hardware from a computer or network without prior notice, effort will be made to inform users within a reasonable time period of any action that is taken.

b. The District may set quotas for disk usage on any of the District information systems.

c. Users who exceed their quota will be advised to delete files to return to compliance.

d. Users may request that their disk quota be temporarily increased by submitting a request to the system administrator stating the need for the quota increase.

e. After fourteen (14) days' notice, the system administrator may remove any excess files.

f. The system administrator(s) may set filters for viruses, SPAM, inappropriate content in email, email attachments and files. Such material may be deleted from the systems by the system administrator(s) without prior notification.

g. The system administrator(s) may block ports on the District firewalls and routers that will prevent certain Internet services from being accessed from District computers. These services would be those deemed to be of little or no educational value and/or those that may compromise network performance or security and/or are illegal.

h. Users may request by letter or email that the system administrator(s) unblock a port.

i. The request must include the educational reasons for the required access and the duration of the access.

j. The system administrator(s) may delete, remove or uninstall any software that is unlicensed or illegal or compromises system or network performance or security without prior notification.

k. The system administrator(s) may remove any electronic device that compromises system or network performance or security from that network system without prior notification.

l. The system administrator may suspend or terminate a user's access to, and use of, any District information system upon breach of the Board policies and administrative procedures.

m. Prior to suspension or termination, or as soon after as is practicable, the system administrator will inform the relevant Principal or department manager, who in turn will inform the user of the suspected breach and give the user an opportunity to present an explanation before deciding on a course of action that is in keeping with Board policies and administrative procedures.

n. Any server-based or Wi-Fi information system must be registered with the Electronic and Computer Services Department. This will allow for the proper configuration on the network system and monitoring of resource utilization.

21. In the event there is a violation of this procedure, the matter will be resolved in a manner consistent with Canadian law, Board policies, this procedure itself, and school-based policy.

22. Liability

a. The user
   i. is liable for the costs of any damage that s/he may maliciously inflict on any District computer system. That damage may include physical damage or electronic damage to system files or data or the files or data of another person using the system;
   ii. may be liable for the costs of repairing any physical damage or the cost of any technical services required to repair a loss of system functions or data.

b. The District
   i. makes no guarantee that the functions or the services provided by or through the District information systems will be error-free or without defect;
   ii. will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions to service;
   iii. will not be responsible for financial obligations arising through the unauthorized use of the system.
   iv. is not responsible for the accuracy or quality of the information obtained through or stored on the system;

References:

- Sections 17, 20, 22, 65, 85 School Act
- Freedom of Information and Protection of Privacy Act School Regulation 265/89
- Policy 131
- BC Education Plan.

- BC Ministry of Education: Internet Safety. http://www2.gov.bc.ca/gov/content/education-training/k-12/support/health-and-safety/internet-safety
- Canadian Charter of Rights and Freedoms
- Canadian Criminal Code
- Copyright Act
- http://www.bewebaware.ca
- Edmonton Public School Board: https://sites.google.com/a/epsb.ca/help-epsb-ca/google-apps/privacy-matters