



Computer and Internet Usage and Access

Purpose

The Board's responsibilities include the establishment of the reasonable boundaries of what is considered acceptable use of the System.

School district network access is provided primarily to support educational research by providing access to unique resources and the opportunity for collaborative work. Access to and participation in the global network known as the Internet carries with it a responsibility for adherence to established guidelines for acceptable use, which are set out in this policy and the procedure below.

Policy

This policy shall govern the use of computer equipment, software, the local and wide area networks (collectively known as the "Network"), e-mail and Internet access provided by the Board of School Trustees of School District No. 34 (Abbotsford), (the "Board") to students, employees, contractors and others.

The District's computers, software, networks, electronic systems and access to the Internet (collectively referred to as the "System") are designed for a very specific and limited purpose. It is intended for educational and/or research purposes and for conducting valid Board business. The District provides access to Internet e-mail capability as well as Internet informational resources, and searching and browsing tools. The District also provides other resources via the Network such as library catalogs and CD-ROM-based materials. Use of the System and access to the Internet for any other purpose is prohibited including, without limitation, commercial, criminal, obscene or illegal purposes. Use of the System to gain access to inappropriate materials, including, without limitation, obscene or pornographic materials, is prohibited.

Procedure

Use of the System

1. Access

- 1.1 Access to the System, including Internet resources is a privilege, not a right. Users must comply with the Computer and Internet Usage and Access Policy and regulations as made by the Board from time to time.
- 1.2 Use of the System requires prior authorization by the Board. The Board reserves the right to restrict the scope of access to individual users or classes of users. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the System.
- 1.3 Authorization for access to the System will be granted only when potential users have signed the required form (*Reference “Computer and Internet Usage and Access Agreement”, PP 9.210-1 and User Agreement, PP9.210-2*) as prescribed by the Board. Students under the age of 19 must have his/her parent(s)/ guardian(s) also sign the form. This form signifies the agreement to be bound by this policy and any rules and regulations respecting the use of the System that are made by the Board from time to time.

Note:

Appendices PP9.210-1, Computer and Internet Usage and Access Agreement, and PP9.210-2, User Agreement will be sent home with students in their school startup registration package at the beginning of school year. The User Agreement is to be signed only once for the duration the child attends a particular school and must be kept on file at the school. In the event the child moves to another elementary school in the District or moves to a Secondary school, then the User Agreement must be re-signed by the student. All new students to the District and any transferring student must sign a User Agreement at their home school.

- 1.4 Students will not be permitted to have remote access to the System or to use the Board’s Internet access from their home or other external locations.

- 1.5 Users of the System will be subject to the School District's and local school's disciplinary process and policies.
- 1.6 The Board will provide students access to the District's own email system on an "as-needed" basis and after the Computer and Internet Usage and Access Agreement (*Reference Form No. 9.210-1*) has been appropriately signed. "As needed" is defined as the reason for requiring access to email for educational and/or research purposes. All student email accounts will be terminated at the end of each school year unless there are special circumstances such as summer programs requiring email access.

2. Purpose

- 2.1 The System is established to enhance the delivery of curriculum as well as to assist in School District business. The System is to be used for educational and career or professional-development activities. School District employees may also use the System to conduct District related business transactions and research.
- 2.2 The purpose of student access to the System is to further the learning objectives of a student's educational program, including, without limitations:
 - providing training in the use of computer systems;
 - providing access to a wide range of material with educational value to the student;
 - facilitating communication with others around the school district and the world to enhance the student's education.

3. System Conduct and Policies

- 3.1 It is important that users conduct themselves in a responsible, decent, ethical, and polite manner while using the System. System users are reminded that speech sent from the System via the Internet will bear the imprimatur of the School District because the domain name (sd34.bc.ca) will be part of the user's Internet address. The following is a list of guidelines whose violation may lead to suspension, termination of privileges, disciplinary or legal action (*see Violation of This Policy – Page 12*).

3. System Conduct and Policies - continued

- 3.2 When interacting on the Internet, you are expected to behave as you would in any other environment where you represent your school/employer.
- 3.3 System users are expected to:
- be polite;
 - use appropriate language (do not swear, use vulgarities, or any other inappropriate language that would normally be against Board and local school rules and policies);
 - obtain permission of the owner of a personal message before re-posting or copying the message to others or to a public forum;
 - obey all copyright laws and any terms and conditions when copying or transferring electronic data;
 - give credit to authors and/or websites when copying their materials found on the Internet.
- 3.4 Users may upload and download public domain programs for their own use or redistribute a public domain program if it is for non-commercial use. However, the user assumes all risks regarding the determination of whether a program is in the public domain.
- 3.5 Users may redistribute non-commercially copyrighted software only with the express permission of the owner or authorized person. Such permission must be specified in the document or must be obtained directly from the author in accordance with applicable copyright laws, Board policy and administrative regulations.
- 3.6 School and student-produced websites created must:
- relate specifically to school activities and programs or student-produced materials;
 - have prior permission to use any content that has not been created by the student or the school;
 - follow guidelines for appropriate content as stipulated in this and other district policies;
 - not contain personal information such as addresses, phone numbers; the full names of students or individual photographs unless written permission is granted by the parent and the student;
 - not contain links to personal (staff or student) homepages;

- be approved by a sponsoring teacher if students produce the web pages.

3. System Conduct and Policies –continued (3.6)

- have parent notification if student materials will be published on the Internet.

3.7 Publications of classrooms, departments, buildings or any other organizational elements of the School District on the System are considered to be publications of School District No. 34 (Abbotsford). The Board has the right to control the content of these publications within the limits of this and other Board policies. Exercising this right may include deletion of materials from these publications as well as other editorial rights.

3.8 Personal web pages may provide links to web pages residing on the System. The Board reserves the right to require the removal of such links if, at the sole discretion of the Superintendent or his or her appointee, any part of personal web pages is deemed to be inappropriate as defined in this policy.

3.9 If a student inadvertently accesses material that is prohibited by this policy or if he or she accesses material that the student is not sure about, he/she must inform their teacher/supervisor of this immediately to protect themselves from disciplinary actions.

4. Prohibited Use — Examples of Prohibited Conduct

4.1 You may not use the System to:

- transmit any materials in violation of Canadian laws;
- duplicate, store, download or transmit copyrighted material that violates copyright law;
- transmit or post threatening or abusive material;
- participate in pyramid schemes.

4.2 Use of the System to submit, obtain, publish, store or display objectionable material is prohibited. Objectionable material includes, but is not limited to:

- information to encourage the use of tobacco, alcohol or controlled substances or otherwise promote any other activity prohibited by Board policy, provincial and federal laws;
4. **Prohibited Use – Examples of Prohibited Conduct – continued (4.2)**
- information or software in violation of any Board policy, local, provincial, or federal law;
 - information encouraging or promoting discrimination towards individuals or groups of individuals based on race, gender, religion or age;
 - information or software that is pornographic or sexually explicit.
- 4.3 You may not violate, or attempt to violate, the security of the System.
- 4.4 You must not vandalize the System. Vandalism is defined as any malicious attempt to harm or destroy data of another member, the Board, or any of the agencies or other networks that are connected to the Internet. This includes, but is not limited to, the uploading or creation of computer viruses.
- 4.5 You may not access another individual's System account or password without his/her knowledge.
- 4.6 When interacting on the Internet, do not:
- use abusive, vulgar, profane, rude, lewd, inflammatory, disrespectful, obscene or other inappropriate language;
 - post criminal skills or speech in the course of committing a crime (e.g. threats to people, instructions on breaking into computer systems, drug dealing, gang activities, child pornography, etc.);
 - use speech that is inappropriate in an educational setting or violates School District Code of Conduct, expectations, and policies;
 - post dangerous information that, if acted upon, could cause damage or present a danger of disruption;
 - re-post personal e-mail that you receive to public forums (e.g., listservs, newsgroups) without the permission of the author.
 - knowingly post or forward false or misleading information.

4. Prohibited Use – Examples of Prohibited Conduct – continued

- 4.7 The System is a shared resource and you should use it in such a way that it doesn't disrupt the services to others. Do not use the System:
- to send chain letters;
 - to play network intensive games;
 - to download excessively large files, except in low use hours;
 - to harass other users. See *Policy No. 9.24, Harassment – Students and Staff*.
- 4.8 The System is not to be used for commercial use. Commercial use is defined as “offering or providing products or services not directly related to school district business”. Unless properly authorized to do so, the use of the System for purchasing products or services is prohibited. The District will not be responsible for financial obligations arising from the unauthorized use of the System.
- 4.9 Provincial and federal laws will govern the use of the District’s System for political lobbying. Use of the System for political fund-raising or other political activities is prohibited. Use of the System for political lobbying is prohibited. Users may use the System to analyze legislative measures and communicate their constructive opinions to elected officials.
- 4.10 The only email services that students may access or sign up for through the system are those authorized by the Manager of ITC or designate.

Responsibilities**1. Overall Responsibilities**

The Superintendent of Schools or designate shall be responsible for the overall system coordination and relationships with regional or provincial programs.

The School District and its employees cannot be responsible for direct supervision of every student while they are using the Internet.

2. System Administration and Maintenance

The Manager of the Information Technology Centre (ITC) shall be responsible for assigning responsibility to ITC staff to maintain and monitor the System.

3. **Building–Level Administrator**

The Building–Level Administrator for schools shall be the school principal. For other facilities, the designated building manager for each facility shall be the Building–Level Administrator.

Administrators will ensure that all of the employees at that location receive instruction in the School District policies, establish a process to ensure adequate supervision and safety of students using the System. The Administrator, in consultation with the area Superintendent or Director, is responsible for conducting building–level activities (such as maintaining and supervising school web pages), maintaining executed user agreements, and applying this policy at the building level.

Prior to posting school websites on the Internet, the sites shall be approved by the area superintendent.

4. **Teachers and Supervisory Staff**

Teachers and other adults who supervise students shall be responsible for educating students about the acceptable and safe uses by providing general supervision and enforcing this Policy.

5. **Parents**

Parents are responsible for ensuring that they fully understand the terms and conditions of the Computer and Internet Usage and Access policy and procedures for the safe use of Internet. (See System Security, Safety and Liability section below.)

System Security, Safety and Liability

1. System Security

- 1.1 Authorized users should not permit other persons to use their access, or account, and should log off immediately after use to ensure that others cannot use their access or account.
- 1.2 Authorized users must not disclose their passwords to any other person except for appropriate business needs. Account holders are responsible for all activity within their account.
- 1.3 Conduct that deliberately or recklessly exposes the System to computer virus infection is prohibited.
- 1.4 System users may not violate, or attempt to violate, the security of the System.
- 1.5 Any attempts to access unauthorized data on the System will result in termination of user privileges.
- 1.6 Any attempts to vandalize System accounts or systems will result in termination of user privileges. Vandalism is defined as any malicious attempt to harm or destroy System equipment or materials, data of another System user, the Board, or any of the agencies or other networks that are connected to the Internet. This includes, but is not limited to, the uploading or creation of computer viruses. Local, provincial or federal law may apply.
- 1.7 Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy or modify the electronic mail of other System users is prohibited as is deliberate interference with the ability of other System users to send and receive electronic mail. Local, provincial or federal law may apply.
- 1.8 System users identifying a security problem on the System must immediately notify the teacher, building-level Administrator or the Manager of the ITC or designate.

2. Safety

- 2.1 There is a wide range of material available on the Internet, some of which may be offensive or conflict with the values of some families. The Board will endeavor to limit access to offensive material, and

may revoke access privileges of students who use the System to access inappropriate materials. However, it is not practically possible for the Board to constantly monitor or individually control student use of the System, nor to prevent inadvertent accessing to offensive material. Parent(s)/legal guardian(s) who have particular concerns about access to inappropriate material should discuss this issue with the appropriate teacher(s) and administrator at their child's school.

2.2 The Board may revoke one or more levels of access of a student at the request of his or her parent(s)/legal guardian(s).

2.3 As a System user, you must not:

- share your password with others except for business purposes. Remember that accounts are to be used only by the owner of the account. Account holders are responsible for all activity within their account;
- distribute or use anyone else's user id and password;
- reveal personal information such as address, phone number(s) or age of yourself, students or colleagues;
- reveal the full names and other personal information of students on web pages that have clear pictures of them.

3. **Liability**

3.1 Financial and Legal Liability

- The district assumes no responsibility or liability for any personal membership or phone charges including, but not limited to, long distance charges, per minute (unit) surcharges and/or equipment on-line cost incurred.
- The Board and Board employees shall not be a party to any such personal transactions or be liable for any costs or damages arising out of, either directly or indirectly, the actions or inactions of sellers.
- The Board will take reasonable measures to prevent student access to objectionable and illegal material from the Internet. However, the Board cannot guarantee that 100% of the materials accessed via the Internet, either intentionally or unintentionally, will not include offensive or illegal contents.

3.2 Liability for Data

- The Board makes no warranties of any kind, whether expressed or implied, for the service it is providing. The Board will not be responsible for any damages users may suffer. This includes, but is not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by the Board's own negligence or user errors or omissions. Use of any information obtained via the Internet is at the user's risk. The Board specifically denies any responsibility for the accuracy or quality of information obtained through its services.
- The opinions, advice, services and all other information expressed by System users, information providers, service providers or other third party individuals in the System and on the Internet are those of the information providers and not the Board.
- It is the responsibility of System users to save electronic mail correspondence they wish saved to their local computer workstation or their personal removable media such as a floppy disk.
- It is advisable that System users make a personal backup of important personal data contained on the System.

3.3 General Liability

The Board does not warrant that the functions or services performed by or that the information or software contained on the System will meet the System user's requirements or that the System will be uninterrupted or error-free or that defects will be corrected. The System is provided on an "as is, as available" basis. The Board does not make any warranties, whether express or implied including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the System and any information or software contained therein.

Privacy and Confidentiality

The Board respects the privacy of System users' e-mail. However, use of the System including Internet access, is neither private nor confidential and may be tracked. Use of the System including the Internet, by any individual, may be monitored or reviewed by the Manager of ITC or designate without prior notice if there are reasonable grounds as described below.

1. The contents of computer hard drives and other storage devices owned by the Board may be examined and read by the Manager of ITC or designate.
2. The Manager of ITC or designate may remove locally posted messages that are unacceptable and/or in violation of the Computer and Internet - Usage and Access Policy.
3. In the case of misuse or suspicion of misuse of the network or services, the Board reserves the right to access any files on the System.
4. The Manager of ITC or designate will not intentionally inspect the contents of users' e-mail, 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 Board, or to investigate complaints regarding mail which is alleged to contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material. The Board will cooperate fully with any participating school district, local, provincial, or federal officials in any investigation concerning or relating to any e-mail transmitted on the System.
5. The Manager of ITC or designate has the right to set quotas for disk/computer usage and download/time limits on the System.

Violations of This Policy

Violations of this policy will be subject to the disciplinary codes set out by the Board and will be handled in accordance with those codes. The appropriate legal authorities will be contacted if there is any suspicion of illegal activity.

Students

Depending on the severity of the violations, discipline for students could lead to suspension of computer use privileges, suspension or expulsion from school.

Principals should refer to “Violation Consequences – Guidelines for Principals”

Employees

Depending on the severity of the violations, discipline for employees could lead to suspension or termination for cause.

Any violations of the Criminal Code will be reported to the police.

Procedure for Suspension or Termination of Access

The Superintendent of Schools and the Manager of ITC or designate has the right to suspend or terminate a user’s access to and use of the System upon any breach of the Computer and Internet 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.

Reference

The following information has been appended to this policy

- *No. PP9.210-1, Internet and Computer Usage and Access Agreement – condensed version of policy*
- *No. PP9.210-2, User Agreement Sign-up form*
- *No. PP9.210-3, Violation Consequences – Guidelines to Principals*

