



POLICY ON THE ACCEPTABLE USE OF INFORMATION TECHNOLOGIES

(Adopted on August 22, 2003 – Revised on November 12, 2010)

(Adopted June 12, 2013)

1.0 GUIDING PRINCIPLES

The Central Québec School Board (CQSB) shall make innovative, creative and responsible use of digital technology to enhance the learning and working environment of all users and will continually re-examine and adapt this policy in order to make appropriate use of constantly changing digital technology.

All employees, commissioners, parents, students or others (users) who have access to electronic systems or devices belonging to the School Board, or personal devices used on Central Québec School Board properties or network, agree to respect the rules as established in this policy.

2.0 LEGAL FRAMEWORK

Civil Code of Québec (R.S.Q. 1991, C-64)

Criminal Code (R.S.Q. 1985, c. C-46)

Act respecting access to information (R.S.Q., c. A-2.1)

Copyright Act (R.S.Q. c. C-42)

Charter of Human Rights and Freedoms (R.S.Q., c. C-12)

Education Act (R.S.Q., c. I-13.3)

Act establishing a legal framework for information technology (R.S.Q., c.32)

Policies and by-laws as adopted by the Central Québec School Board

Québec Education Plan

Collective agreements and Regulations governing working conditions

3.0 WHAT IS COVERED BY THIS POLICY?

The purpose of this policy and the appendices that accompany it, is to establish guidelines and responsibilities related to the use of technology for all users, using equipment and facilities owned or leased and operated by the CQSB and/or personally owned equipment used to access the School Board's network. It also applies to anyone whose conduct using the network or internet, in or outside school board premises, has a negative impact on the CQSB.

This policy governs the use of electronic systems and devices listed below.

This list is not necessarily exhaustive.

- Electronic communication, such as e-mail, video conferencing, on-line collaborative tools (i.e. Google docs), social networking services;
- Handheld devices, such as cell phones, electronic tablets, personal music players;
- Pagers, telephones, voice boxes, facsimile machines (fax);
- Computers and their peripheral equipment;
- Electronic/digital recording devices, such as cameras, cell phones;
- Internet;
- Electronic files;
- The use of information saved, communicated, or treated by any of these systems.

4.0 DEFINITIONS

The definitions to be used in the interpretation of this policy may be found in Appendix 1 to this policy.

5.0 CONTENT

Ownership

- 5.1** The Central Québec School Board is the owner of all information and messages that are created, sent, received, saved, or accessible on the School Board's electronic systems available to users, unless such information is subject to dispositions of the Copyright Act.
- 5.2** The Central Québec School Board maintains the right to verify and destroy any information or message that does not conform to this policy as provided for in section 17, Roles and Responsibilities.
- 5.3** The Central Québec School Board is not responsible for personal electronic systems or devices that individuals bring to school or to work and cannot be held responsible in the event of loss or theft. In the event that a device is confiscated, the school and School Board become responsible for its safekeeping.

6.0 USE OF INFORMATION TECHNOLOGY/DEVICES AND PROHIBITED ACTIVITIES

Every user has access to the information technologies of the School Board within the confines of his functions.

Personal use of electronic systems is permitted within the following parameters:

- 6.1** Information technologies may be used for personal purposes within the confines of this policy and outside of working hours or during scheduled breaks. The School Board reserves the right to withdraw or limit this privilege.
- 6.2** Students may use information technologies and devices according to the rules established in each school/centre and in conformity with this policy. The use of personal devices is to be approved by school/centre administration.

- 6.3 Users may not use any information technology or device for personal purposes in a manner that will incur a cost to the School Board.
- 6.4 Users are responsible for properly using all Central Quebec School Board's electronic systems and devices.
- 6.5 The School Board reserves the right to determine appropriate applications and sites to be used within the School Board. The Information Technology Advisory Committee (ITAC) and/or the Administrative Users Committee will make recommendations to the Director General in this regard.
- 6.6 Removal from the premises of the School Board, lending or borrowing of information technologies or devices must be pre-authorized by the immediate supervisor.

7.0 RESTRICTIONS CONCERNING THE CONTENT OF MESSAGES

Communications via information technologies and devices must not be defamatory, offensive, harassing, or disturbing. In addition, communications must not contain images or comments of a sexual or racist nature nor any other images or comments based on age, race, colour, sex, pregnancy, sexual orientation, civil status, religion, political beliefs, language, ethnic origin, social condition, or handicap.

The Québec Civil Code and the Charter of Human Rights and Freedoms legislate the producing, posting and use of a person's voice and or image in any fashion.

In addition to the legal interpretation and sanctions, these types of communications can be sanctioned under the School Board's Harassment Policy as well as the school/centre's Rules of Conduct and are considered to be cyberbullying.

8.0 PROHIBITED ACTIVITIES

Users of information technologies may not engage in any activities that might compromise the reputation of the School Board or any individual. A non-exhaustive list of prohibited activities may be found in Appendix 2 to this policy.

9.0 CONFIDENTIALITY

Communications on electronic systems are not private and their security cannot be guaranteed. Passwords and user codes are assigned with a view to protecting the confidential information belonging to the School Board against third party interference and not to confer confidential status on users' messages.

- 9.1 When navigating on the Internet, users must remember that sites visited may be verified and compiled for control purposes;
- 9.2 Users must presume that any communication, personal or not, that is created, sent, received, or saved on the School Board's electronic systems may be read or heard by someone other than the person for whom the message was intended;

- 9.3** In order to protect the School Board's electronic systems and the information contained therein, users must not use applications that are not supported by the School Board to encrypt their email, voice box, or any other information contained on or transmitted by the School Board's systems unless prior approval is obtained.
- 9.4** In order to ensure confidentiality of messages sent by e-mail or facsimile machines (fax), the following text should appear in the message: "Confidentiality notice: This communication may contain privileged or confidential information. If you are not the intended recipient or received this communication by error, please notify the sender and delete (destroy) the message."

10.0 INSPECTION OF MESSAGES

The School Board reserves the right to inspect, access, recuperate, read, and reveal communications in certain circumstances when:

- 10.1** It is necessary and legitimate to protect the interests of the School Board;
- 10.2** The School Board has reasonable doubt that a user's activities on the electronic systems are or are about to be inappropriate;
- 10.3** The School Board must examine the content of messages to obtain information that is not otherwise available;
- 10.4** Required by law or by a court order when there is reasonable doubt that a user of the electronic systems is or is about to carry out or commit an act that might cause prejudice, either directly or indirectly, to the School Board;
- 10.5** The user is not available due to death, sickness, vacation, or is no longer in the employ or registered with of the School Board;
- N.B.** In the event that the user leaves the School Board, the School Board reserves the right to maintain that person's electronic address for a pertinent length of time after his departure so that important communications may be transmitted to the School Board.

The results of periodic inspections will remain confidential unless further action is to be taken under the dispositions of this policy.

11.0 PROTECTION OF INFORMATION

It is prohibited to transmit confidential information to employees of the School Board or to anyone else who is not entitled to access that information unless specific authorisation has been obtained from the Secretary General and the third party gives written agreement not to divulge the information and that the agreement is approved by the School Board's legal advisors.

Users must destroy messages that they do not wish to keep in a timely manner. The School Board is responsible for the destruction of archived material according to the stipulations of the conservation calendar. The School Board is responsible for ensuring that confidential information held by a person who has left the School Board is archived or destroyed in the appropriate manner.

12.0 INFRINGEMENT

Any infringement of the stipulations of this policy, including infringement of the rules concerning confidentiality and security, may lead to the suspension of the privilege of access to the School Board's information technologies, disciplinary measures, reimbursement of costs incurred to the School Board, and if necessary, dismissal in accordance with the relevant collective agreements and regulations governing working conditions.

13.0 ARCHIVES

Information contained in an electronic file must be saved, filed and archived according to the CQSB Records Retention and Management Policy.

14.0 MALWARE AND UNLAWFUL ALTERATION

All files downloaded from the Internet or any storage media must be submitted to a malware detector prior to being used. It is expressly prohibited to deliberately introduce a malware, to attempt to break through security systems, or to proceed with unlawful alterations using the electronic systems of the School Board.

Users must not deactivate security systems that have been put in place or attempt to circumvent them. Users must immediately report the existence of a malware, any unlawful alteration, and any other infringement to this policy, to their immediate supervisor who will inform the coordinator of the information technologies department, if necessary.

15.0 ONLINE PURCHASING

The School Board's administrative procedures and Policy on Supply, Services and Construction Contracts apply to all online purchases made through the School Board's electronic systems.

16.0 AGREEMENT

All users agree to abide by the terms of this policy according to the modalities adopted by each school, centre, and service. In the absence of a policy in a school, centre, or service, this policy applies.

17.0 ROLES AND RESPONSIBILITIES

17.1 Council of Commissioners

Adopts the Policy on the Acceptable Use of Information Technologies.

17.2 Director General

Ensures the application of the Policy on the Acceptable Use of Information Technologies.

Ensures that access to information technologies is suspended when necessary.

Reserves the right to hire a qualified person to examine the School Board's electronic systems.

Authorizes the verification, inspection and/or destruction of information when the information or message does not conform to the Policy.

17.3 Secretary General

Ensures that the laws and regulations involved in the application of this policy are respected.

Ensures that information is protected according to the law and authorises the transmission of information in accordance with the law.

17.4 Director of Information Technologies

Acts as Chairperson of the ITAC and oversees the revision of the Policy on the Acceptable use of Information Technologies.

Acts as a liaison between the ITAC and the AC.

17.5 Information Technologies Coordinator

Acts as administrator of the information technologies network and, upon the request of the Director General, may suspend access to information technologies.

Will only carry out inspections as provided for in section 10, at the request of the Director General.

17.6 School and Centre Principals and Directors of Service

Ensure that all employees and other users under their jurisdiction are aware of the Policy on the Acceptable Use of Information Technology.

Ensure that the stipulations of this policy are respected and that access is suspended when necessary.

Ensure that the appropriate security systems are in place and functional.

17.7 Users

Must provide their immediate supervisor with their user code and password for the systems that they use, in a confidential manner, when requested.

In the case of students working on information technologies in a school or centre, the immediate supervisor is the teacher responsible for the class.

Must abide by the rules established in this policy.

18. APPLICATION

This policy is effective on the date of its adoption by the Council of Commissioners. The policy will be reviewed annually or as needed.

DEFINITIONS

- **Cyber bullying:** Any repeated direct or indirect behaviour, comment, act or gesture, whether deliberate or not, including in cyberspace, which occurs in a context where there is a power imbalance between the persons concerned and which causes distress and injures, hurts, oppresses, intimidates or ostracizes.
- **Discussion group:** A group of people who use the Internet to discuss a topic (blog, chat).
- **Electronic mail or email:** A message sent through an electronic network, handheld or electronic device.
- **Employee:** Any person who is hired and remunerated by the School Board.
- **Handheld devices:** Any portable device which can either connect via cellular technology, wireless internet connection (wi-fi) or other, or which can take pictures, videos or voice record. These devices can be property of the School Board or personal.
- **Electronic devices:** Any information technology (IT) component which can be found in the School Board's schools, centres or offices.
- **Information contained** Information in the form of text, symbols, numbers, in an electronic file: pictures, sound or images for which the access, storage, treatment, or communication is only possible through the use of information technologies.
- **Information technology:** The materials, software, and services used for the creation, collection, treatment, and transmission of information.
- **Malware:** Short for *malicious software*, is designed to infiltrate a computer system without the owner's informed consent.
- **Personal Network:** Network other than the one supplied by the CQSB.
(i.e. mobile networks: 3G, 4G, LTE and personal wifi)
- **School Board:** The Central Québec School Board.
- **Service Provider:** A natural or legal person who provides services of a technical nature or professional services.
- **Social Networking:** Activity defined by utilizing internet sites , Programs, services or platforms which facilitate building and maintaining relationships by exchanging messages, photographs or other electronic files, which are automatically distributed over the internet or other network.

- Supplier: A natural or legal person who provides goods.
- Upload or download: The transfer of stored information or programs between a local computer and a distant computer through an electronic network.
- User: Any employee, commissioner, parent, student, or other person who uses or has access to the School Board's electronic systems.
- Voice-over IP: Technology that allows voice (phone calls) to be carried using computer networks (local network or internet).

Non exhaustive list of prohibited activities for users of information technologies as per section 8 of this Policy.

Users of information technologies and devices may not :

1. Use software without a license;
2. Attempt to infiltrate another computer;
3. Hold, distribute, look at, or exchange pornographic, obscene or heinous material;
4. Send message that might be interpreted to be discriminatory or harassment; In this case, the sanctions will be linked to the CQSB's zero tolerance policy regarding harassment;
5. Carry out any illegal activity;
6. Create or distribute chain letters not related to the activities of the School Board;
7. Express opinions related to political beliefs or religious propaganda in a manner which would indicate that they are the opinions of the School Board;
8. Carry out solicitation not related to the activities of the School Board;
9. Send publicity not related to the activities of the School Board;
10. Send messages related to union activities unless a special agreement has been concluded according to the specifications of the relevant collective agreement;
11. Participate in gambling or betting;
12. Register in mailing lists not related to School Board activities;
13. Post, without the authorisation of their immediate supervisor, information, opinions, or comments in discussion groups or on electronic bulletin boards;
14. Upload or download, transmit, or distribute unlawfully any material subject to a patent or protected by copyright or a trademark;
15. Upload or download, transmit, or distribute any information or document, confidential or private, without prior authorisation from the School Board or other relevant authority;
16. Access information technologies without authorisation, wilfully damage, alter, or cause a malfunction of these information technologies in any manner such as the installation of a screen saver or other software;
17. Employ another person's user name or password or reveal user codes or passwords, including one's own unless expressly authorised to do so;

18. Allow a third party to access or to use the electronic systems of the School Board, to gain access to confidential information or otherwise compromise the security of the electronic systems or use the systems on behalf of a third party without authorisation;
19. Open email messages addressed to someone else or access someone else's voice box;
20. Send anonymous messages;
21. Create telecommunication links without authorisation such as chat, voice-over IP;
22. Photograph, record, either by video or audio, any individual without their consent.

Parent / Guardian Consent (Users under 18 years of age must have parent/guardian consent)

As the parent / guardian of the above named student, I have read and understand the above rules and know that I have online access to the complete Policy on the Acceptable Use of Information Technology at www.cqsb.qc.ca or at my student's school. I grant permission for my son / daughter to access networked services such as e-mail and the Internet.

Name of Parent / Guardian (Please print): _____

Signature of Parent / Guardian: _____

Date: _____



Publication of Student Work, Photographs and Parent Consent

Students may have their names, photographs, texts, artwork, video, audio, or other derivative works published in the school and elsewhere. This means that your son/daughter's name will be available to the general public. Permission to do so must be obtained from the parents of the student under 18 years of age or from the student if 18 years of age or more.

Student acknowledgement and signature:

I have read the **Policy on the Acceptable Use of Information technologies** and understand the rules concerning use of Internet and school computer facilities, more particularly for this section, the importance of respecting other users, and agree to abide by them.

Name: _____

Signature: _____

School: _____

Date: _____

Age: _____

Homerroom: _____

Parental consent and signature:

I give permission for my son/daughter's name, photographs, footage, video clips and/or work to be released for publication in the school and *in the following*:

- | | | | |
|--|---|--|--|
| <input type="checkbox"/> Yearbook | <input type="checkbox"/> School Photos | <input type="checkbox"/> Web page | <input type="checkbox"/> School newspapers |
| <input type="checkbox"/> Local newspaper | <input type="checkbox"/> Radio | <input type="checkbox"/> Television | <input type="checkbox"/> Special school projects |
| <input type="checkbox"/> Vide Conferencing | <input type="checkbox"/> Internet communications (i.e. Skype) | <input type="checkbox"/> Blogs, Pod Casts, Wikis | |

Printed name : _____

Relationship to student : _____

Parent / Guardian signature : _____

Date : _____

I DO NOT give permission for my son/daughter's name, photographs, footage, video clips and/or work to be released for publication.