commission scolaire
DU LITTORAL

IDENTIFICATION CODE
POL16-030

TITLE: COMPUTER AND NETWORK USAGE POLICY

EFFECTIVE DATE	REQUIRED AUTHORIZATION	FOLLOW-UP RESPONSABILITY
September 7th, 2010	Administrator	Person responsible of IT

ROAD MAP

	DATE	AUTORIZATION
ADOPTION	September 7th, 2010	Ordinance 10-077
UPDATE	May 29th, 2014	Ordinance 14-041
LAST UPDATE	April 28th, 2016	Ordinance 16-030

Table des matières

commission scolaire DU LITTORAL

1. PREAMBLE

The Littoral School Board acknowledges the importance for its students and staff to have access to computer equipment and a telecommunications network. The School Board grants this privilege for teaching, learning, research, management and administrative activities as well as for services related to the School Board's mission.

As the owner and manager of computer equipment and resources, the School Board must ensure that their use and information process, as well as the use of the network, comply with certain standards.

The School Board requires that the use of computer resources and the telecommunications network comply with the School Board's and its institutions' educative and administrative objectives.

Beyond the provisions contained in the present policy, the School Board expects each person's usage to be governed by rules of conduct and by Quebec and Canada laws and regulations.

2. POLICY GOAL

2.1 This policy seeks to establish the School Board's regulations regarding the use of electronic systems, including and without limitations:

- Electronic mail
- Telephones
- Voice mailbox
- Fax machines
- Computers and related equipment
- Internet
- Intranet
- Computer-based files
- Use of stored, disseminated or processed information through these systems

2.2 All abovementioned employees and other workers who use or have access to the School Board's computer and electronic systems accept to comply with the regulations set forth in this policy.

3. LEGAL FRAMEWORK

- An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information (R.S.Q. chap. A-2).
- Copyright Act (R.C.S. chap. C-42).
- Loi sur les droits d'auteurs et les établissements d'enseignement (Direction des ressources didactiques du ministère de l'Éducation).
- Civil Code of Québec.

4. DEFINITIONS

4.1 **Computer Network Administrator:** Any person working for the School Board who is responsible for controlling and managing the computer resources and telecommunications network, in whole or in part.

4.2 **Bandwidth**: In the computer field, bandwidth indicates the flow of information on the network, measured in megabits (Mbps). (Source Wikipedia).

4.3 **School Board:** the Littoral School Board.

4.4 **Electronic Communication:** Any sharing of information through technology assets.

4.5 **Email:** A computer-sent message.

4.6 **Courseware:** Software made for the specific purpose of computer-assisted teaching.

4.7 **Copyright:** Signifies that all the rights vested by the *Copyright Act,* especially the exclusive right of the owner of that right to publish, produce, reproduce, represent or execute in public, through telecommunication or otherwise, to translate or adapt, in any form, his or her work or an important part of it, or to allow someone else to do so. **Performing one of these acts without the consent of the owner of that right constitutes a violation of copyright.**

4.8 **Discussion forums or Focus groups:** A group of people who use Internet or Intranet to exchange directly or offline words on a common subject.

4.9 **Internet or Internet Network:** A worldwide computer network comprised of national, regional and private networks which are bound by a TCP/IP link protocol and cooperate in order to offer an interface to their users.

4.10 **Intranet or Intranet Network:** A private computer network which uses certain or all link protocols and Internet network technologies.

4.11 **Software:** All programs destined to process a computer in a given fashion.

4.12 **Netiquette**: Rules of etiquette governing Internet users' behaviour on the network, mainly during sharing on forums or through email.

4.13 **Work**: Refers to all literary, dramatic, musical or artistic work, data or data bank (written text, sound, symbolic or visual), show presentation or any other work defined in the *Copyright Act*, whether this work is conventionally-based (book, soundtrack, videocassette), computer-based (diskette, CD-ROM, software, hard drive) or accessible through Internet.

4.14 **Software Package**: All documents and programs designed to be provided to many users, for the purpose of the same application or function.

4.15 **Personal Information**: Information pertaining to a physical person that allows his or her identification, in compliance with the provisions contained in the Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information

4.16 **Computer Network or Telecommunications Network:** all material and software implemented to ensure communications between computers.

4.17 **ICT (Information and Communication Technologies) including**: servers, computers, computerized workstations and their units or reading, storage, reproduction, printing, transmission or reception peripheral accessories, or any telecommunication equipment

including voice-communication equipment, software, software packages, courseware, data banks (written text, sound, symbolic or visual) integrated into equipment or a computer medium, email or voice mail systems, or into a website or internal or external computer network owned, rented, controlled or managed by the School Board or on which it has a right of use.

4.18 **FTP site**: A website where data is stored and files can be transferred thanks to FTP protocol.

4.19 **Website**: A website where data is stored and accessible through the Web.

4.20 **Download:** Downloading stored data or programs between a remote computer and an on-site one through an electronic network.

4.21 **User**: A user or staff member, young or older student, supply teacher, parent of a student as well as any other natural or legal person using or authorized to use ICT.

5. OBJECTIVES

This policy states the terms of use of the equipment, computer resources and network.

Its goal is to protect collective investments, as well as students and staff against misuse or illegal use of the computer equipment at their disposal. It should not be considered as an attempt to criticize users' work.

The objectives of this policy are to:

5.1 Promote a responsible use of ICT.

5.2 Contribute to the achievement of the educational mission.

5.3 Preserve the School Board's integrity as a responsible educational body.

5.4 Prohibit the misuse or illegal use of ICT by users.

5.5 Ensure the protection of personal information.

5.6 Establish markers for the use of ICT for personal purposes.

5.7 Minimize the risk of destroying or modifying systems and data.

5.8 Foster the compliance with regulations governing information confidentiality.

5.9 Ensure the safe use of the School Board's ICT systems.

6. GENERAL CONSIDERATIONS

6.1 Scope

6.1.1 The present policy applies to users of the School Board's ICT resources, students, younger or older, staff members, managers, trainees, volunteers and members sitting on different committees, as well as to any other person having access to the School Board's telematics resources.

6.1.2 It applies to their professional or personal activities, irrespective of where these activities take place, and covers all gathered, processed or recorded data, and input on any type of medium.

6.1.3 Computer science, telecommunications and Internet are indispensable tools to the achievement of the School Board's educational mission. However, these tools also contain

inherent dangers we need to protect ourselves from: the technology surrounding Internet leads to the censorship of the content the users have access to.

6.2 Priority of Use

6.2.1 ICT resources are at the disposal of users for teaching, learning, management and administrative activities, as well as community services related to the board's mission and to that of its institutions, within the duties of each of its users.

6.2.2 Only duly authorized users can have access to and use ICT resources, within the limits of the authorization granted to the user by the School Board.

6.2.3 For students, Internet network use is allowed according to internal regulations and in compliance with the provisions of the present policy.

6.2.4 Use of the School Board's electronic systems must be done within the framework of his or her duties.

6.3 Property Rights

6.3.1 The Littoral School Board owns all information or messages created, sent, received, stored or accessible through its electronic systems, within the users' duties.

6.3.2 The Littoral School Board has a limited right to verify or destroy any information or message which does not comply with the present policy.

6.4 Personal Use

The use, for personal purposes, is allowed within the following limits:

6.4.1 For staff members, the Internet network can be used with the authorization of the immediate superior, outside working hours, and under the conditions provided by the present policy. The School Board reserves its right to withdraw or limit this privilege.

6.4.1.1 To prioritize educational needs, the School Board reserves its right to limit, at all times, the use of bandwidth.

6.4.2 Users can use the School Board's technology assets for personal use, under certain conditions, if:

6.4.2.1 Their use does not interfere with the employee's work or that of other employees.

6.4.2.2 Their use does not interfere with the student user's educational activity or that of other students.

6.4.2.3 The user pays, if appropriate, the user fees for the use of equipment or material.

6.4.2.4 The user respects the legal use of the material and will not conduct commercial activities.

6.4.3 The user pays the incurred costs for the restoration of equipment to their initial condition.

6.4.4 The user pays the value of the lost or broken equipment according to the cost estimated by the School Board.

7. DESIRED ETHIC

The user of the School Board's ICT acts in a way to:

7.1 Respect people, their private lives, and the personal or confidential information concerning them when communicating through messages or images.

7.2 Respect the institution's education project.

7.3 Respect copyright and the intellectual property of others (see section 12).

7.4 Respect the security measures implemented by the School Board.

7.5 Comply with netiquette regulations.

7.6 The forbidden behaviors mentioned in this policy define the acts that would be contrary to the School Board's desired ethic regarding the use of technology assets, but this enumeration should not be considered as exhaustive.

8. OBSERVANCE OF THE SCHOOL BOARD'S EDUCATIONAL MISSION

8.1 Forbidden Behavior

Any use of the School Board's technology assets for non-authorized or illegal purposes is strictly forbidden, especially:

8.1.1 To download, consult, store and disseminate folders containing words or images which are gross, defamatory, offensive, troubling, disparaging, or discriminatory based on race, color, gender, sexual orientation, civil status, religion, political convictions, language, age discrimination or in any way contrary to the School Board's or its institutions' educational mission.

8.1.2 To download, consult, store and disseminate folders containing words or images which are heinous, violent, indecent, of pornographic nature, racist or in any way illegal or incompatible with the School Board's or its institutions' educational mission.

8.1.3 To download, consult, store and disseminate information which could lead to the creation of explosive devices or substances, or substances or devices causing injury to others.

8.1.4 To use technology assets for propaganda, discrimination or harassment purposes, or to utter threats, of any form, for joking or cyber bullying purposes.

8.1.5 To use technology assets to send advertisements and promote or make transactions as the owner of a business.

8.1.6 To participate in the gambling or lottery of any kind.

8.1.7 To participate in piracy (music, games, software, etc.) or the intrusion or blocking of computer system activities.

8.1.8 To use technology assets to adversely affect someone's reputation.

8.1.9 To associate/post personal comments, in the School Board's or its institutions' name, in group discussions or chatting sessions on bulletin boards, or use any other method of opinion sharing in a way to let believe that the opinions expressed therein are endorsed by the School

Board or its institutions, unless when done by someone authorized to do so within the performance of his duties.

8.1.10 It is forbidden to chat on Internet unless this action is done during a highly supervised educational or extracurricular activity, or when required for administrative purposes.

8.1.11 It is forbidden to participate in Web-based group games unless this participation is done during a highly supervised educational or extracurricular activity which takes place in a context ensuring the security of technology assets, the network and the intellectual property, and respects the school's lifestyle.

8.1.12 It is forbidden to engage in costs directly from the School Board's resources.

8.2 Forbidden Activities

Any user of the School Board's electronic systems cannot use them in a way to compromise the School Board's reputation, for example:

8.2.1 Use an illicit copy of software.

8.2.2 Install non-authorized/unknown software to the School Board.

8.2.3 Try to infiltrate other computers.

8.2.4 Perform illegal activities.

8.3 It is <u>expressly forbidden to</u> use the School Board's electronic systems to:

8.3.1 Solicit activities which are not School Board related.

8.3.2 Appear on a mailing list unrelated to the School Board's activities.

8.3.3 Do clandestine work.

8.3.4 Illegally download, send or distribute proprietary or protected hardware by copyright or trademark.

8.3.5 Use the user name or password of another person or disclose a code or password, including your own, unless duly authorized.

8.3.6 Send anonymous messages.

8.3.7 Open, without authorization, someone else's email or access someone else's voice mailbox.

8.3.8 Use personal devices on the School Board network without authorization and for personal use.

9. HARMFUL CONDUCT TOWARDS THE ICT SERVICE

9.1 It is strictly forbidden to intentional act in a way to interfere with the proper functioning of technology assets, among other things, to insert or spread a computer virus, to destroy or modify data or software and use access codes or passwords belonging to others without authorization, or to act in a way to deactivate, challenge or bypass any of the School Board's security systems.

9.2 It is strictly forbidden to install or patch equipment which has not been authorized by the IT service, such as wireless terminals or other equipment which could infiltrate or access the School Board's electronic systems.

9.3 All non-authorized and exposed equipment will immediately be confiscated.

10. NON-AUTHORIZED ACCESS

Unless authorized, it is strictly forbidden to access or try to access files, data banks, systems and internal or external networks whose access is restricted or limited to a specific category of users.

11. REASONABLE USE

When equally sharing resources, the user cannot monopolize or overuse the technology assets or the bandwidth, by over storing information or using Internet to listen to the radio or watch a program which is not part of an educational activity.

12. COPYRIGHT AND INTELLECTUAL PROPERTY

12.1 General Rule

12.1.1 At all times, the user must respect copyright and other intellectual property rights of third parties.

12.1.2 The following documents are examples of documents that are likely to be protected by copyright and other intellectual property rights: the content of email, its textual content, the graphics and sounds of a website, music, pictures or graphic designs available on the Web, software downloaded from an FTP site, the use of a logo or a trademark.

12.1.3 In certain circumstances, the following actions might violate copyright or intellectual property rights: downloading a file, digitalizing a printed document, retouching pictures or the text of a third party, broadcasting music on the Web or posting a third party's artistic work when protected by copyright.

12.2 Copy of software, software packages and courseware

Reproduction of software, software packages and courseware are only authorized for copy security purposes by the IT service or under user license standards that govern them.

12.3 Prohibited Behavior

It is strictly forbidden for users to:

12.3.1 Use an illegal reproduction of a software or electronic file.

12.3.2 Participate directly or indirectly in the reproduction of an illegal software or electronic file.

12.3.3 Modify or destroy a software, a data bank or an electronic file, or to access them without the owner's authorization.

12.3.4 Reproduce software-related documents without the copyright owner's authorization.

12.3.5 Use technology assets to commit or try to commit an offence in violation of copyright and intellectual property laws.

13. ELECTRONIC MAIL

13.1 Identification

For all electronic mail broadcasted on the network, the user must use the School Board's email address, identify him or herself as the signatory of the message, and if applicable, indicate his or her title.

13.2 Respecting Confidentiality and Integrity of Messages

The user must respect, when applicable, the confidentiality of messages being sent on the network and refrain from intercepting, reading, modifying or destroying any message not destined to him.

13.3 Forbidden Behavior

It is strictly forbidden for users to:

13.3.1 Use one or many quirks or other means to send an email anonymously or using another person's name.

13.3.2 To send, to staff members or groups of staff members, messages concerning different topics, news of all sorts, chain letters or any non-relevant information about the School Board or its institutions' activities which would monopolize the telecommunication network's bandwidth.

14. CONFIDENTIALITY AND PROTECTION OF PERSONAL INFORMATION

14.1 Confidential Information

The information contained in the technology assets is confidential when it has the characteristics of personal information or information protected by the School Board under the Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information, or information pertaining to a person's privacy provided by the Civil Code of Québec.

14.2 User's Obligations

14.2.1 Observance of Protection Mechanisms

The user must observe the rules established by the School Board and that pertain to the conservation, access, transmission and dissemination of personal information through technology assets.

14.2.2 Dissemination of Personal Information

The user cannot disseminate, without the consent of the people concerned, personal information in the form of written information, pictures or other visual documents showing the people doing activities and allowing them to be identified by their name. When the user is a student, he must be informed of the conduct to adopt when transmitting personal information concerning him or members of his family, friends or any other person.

14.2.3 Access Code

Notify the IC Service of any irregularity concerning your access code.

Also, you should regularly change your passwords and make sure they are kept confidential according to the procedure you will be given by the IC Service.

14.3 User's Right to Confidentiality

14.3.1 The School Board respects the privacy of users. However, given technology assets are available to users to contribute to the School Board's mission and that of its institutions, the user's privacy is limited. Therefore, equipment, systems, and work files must be accessible at all times by management or the computer network administrator.

14.3.2 The user must know that the School Board could be called, during legal proceedings, to enter into evidence the content of any document stored in computer mediums it owns. In such a case, the School Board reserves its right and possibility to enter any system without prior notice to inspect and control all data it contains.

15. RESPONSIBILITIES

15.1 Losses, Damages or Inconveniences

The School Board assumes no responsibility, direct or indirect, for losses, damages or inconveniences caused to users while or after using technology assets, or in the case it should, for any reason, reduce or interrupt its services, for whatever length of time, or even definitely cease its activities.

15.2 Illegal Acts

The user is responsible for his actions when using the School Board's technology assets. The user who commits an illegal act could be prosecuted or sued for damages.

16. EMERGENCY AND SAFETY MEASURES

16.1 Verifications

16.1.1 The School Board reserves its right to maintain a record of transactions made with its technology assets and its telecommunication network and to analyze the information contained in those records to target non-authorized and illegal activities on its network.

16.1.2 Service and institution management are authorized, at all times and without prior notice, to proceed with verifications deemed necessary and make and keep copies of documents, data or information to ensure the compliance with the provisions herein, as well as the instructions and regulation issued by the School Board to ensure the enforcement of the School Board's agreements and relevant protocols, or provincial and federal regulations.

16.1.3 The computer network administrator can make verifications, without prior notice, when an emergency situation arises; for example, detect the presence of a virus in the network or the overuse of the network's resources.

16.1.4 The School Board reserves its right to remove from its technology assets any illegal content or content that violates the provisions contained in this policy.

16.1.5 The School Board reserves its right to monitor, access, retrieve, read and disclose communications in certain circumstances when:

16.1.5.1 The School Board has reasonable grounds to believe a user is behaving or about to behave inappropriately with the School Board's electronic systems.

16.1.5.2 The user is unavailable for reasons of death, illness, vacation or is no longer employed by the School Board.

16.1.5.3 If a user leaves the School Board, the latter reserves its right to keep the user's email for a period it deems appropriate, following his or her departure, to ensure that important communications be sent to the School Board.

16.2 Suspension of access rights during verification

A user's access rights can be suspended for the duration of verification. Such a decision is made by the administrator, the department director or the institution principal.

16.3 Security

The IT Service offers computer tools that ensure:

16.3.1 The security of technology assets.

16.3.2 The protection against viruses, intrusions or data alterations.

16.3.3 The prevention of illegal uses.

The School Board can establish instructions and regulations to ensure the security of technology assets, and proceed periodically to verifications of that nature.

16.4 File Storage

As in the case of documents created, received and filed by a user in a physical file, it's each user's responsibility to ensure that all documents received are on a computer medium, kept and saved according to the regulations established by the School Board regarding file storage. Messages that are not to be saved should be disposed of according to same regulations.

16.5 Viruses and Illegal Alterations

Any file uploaded from Internet or any removable medium must be scanned by an antivirus software before its use. It is explicitly forbidden to deliberately introduce viruses, try to breach security systems or perform illegal alterations with the School Board's electronic systems.

The users cannot deactivate the security systems put in place or try to bypass the security measures put in place. The users have to immediately report the presence of viruses, any illegal alteration or other offence to the immediate superior who will, when applicable, ensure the follow-up with the computer network administrator.

17. SANCTIONS

17.1 Penalties and Sanctions

The user who violates the provisions of this policy or the instructions and regulations issued by the School Board to ensure its enforcement, can be subjected to the penalties and sanctions provided by relevant laws and regulations, the disciplinary measures provided by the regulations and collective agreements protecting staff members and the agreements provided by an institution regarding the rules of conduct and behavior students have to abide by. These measures can lead to a discharge or expulsion.

17.2 Also, one or many of the following administrative sanctions could apply:

17.2.1 The cancellation of user access codes and passwords.

17.2.2 The prohibition to use in totality or in part, technology assets, including to access computer labs.

17.2.3 The destruction, without prior notice, of files created contrary to this policy, illegally or containing information of illegal nature.

17.2.4 The obligation to reimburse the School Board any sum it would have been called to pay in damages, penalties or otherwise, following a violation.

17.2.5 The use of personal devices (iPhone, iPad, other tablets...) by students (or the personnel) during class hours is prohibited. See Annex A for an example of sanction.

17.2.6 Each school has a procedure to follow for students who do not respect this policy.

18. ROLES AND RESPONSIBILITIES

18.2 The Administration

18.2.1 Ensures the enforcement of the present policy. and has the authority to suspend access privileges to the electronic systems when necessary.

18.2.2 Reserves its right to hire, if required, any other worker capable of monitoring the electronic systems.

18.3 Information Technologies Service

18.3.1 Acts as the computer network administrator, and upon request, can suspend the access privileges to the electronic systems.

18.3.2 Is responsible for relevant documents and the enforcement of the laws and regulations targeted by the enforcement of this policy. Must ensure the protection of the information and of its dissemination throughout the corporation, if applicable.

18.3.3 Can do the monitoring provided by section ---after having informed the human resources branch.

18.3.4 Issues virus alerts when necessary.

18.4 Center, Service and School Managements

18.4.1 Ensure all the employees and workers are aware and adhere to the present policy.

18.4.2 Ensure the safe working conditions of the electronic systems under their responsibility.

18.4.3 See to the respect of the terms of the present policy and act appropriately in the event of abuse or non-compliance.

18.4.4 Ensure that access privileges to the electronic systems are suspended when necessary.

18.4.5 Insert certain elements of this policy in the local codes of conduct.

18.5 Users

18.5.1 Must give their immediate superior, confidentially, when required, the codes or passwords needed to access the systems they use.

18.5.2 In the case of students working on electronic systems at school or at the center, the immediate superior is the teacher responsible for the group in question.

18.5.3 Must accept the policy's regulations concerning the use of electronic systems.

19. APPLICATION

19.1 The person responsible of IT is responsible for the enforcement of the present policy and the latter comes into force when adopted by ordinance.

19.2 He exercises this responsibility in collaboration with the administrative unit directors (services, school and centres).

20. EFFECTIVE DATE

The present policy comes into effect on the day of its adoption.

ANNEX A

USE OF PERSONAL DEVICES

The use of portable technology is a very real part of our everyday lives, however it is important to ensure that it is used to enrich the learning environment for everyone. There are a number of existing and emerging technologies (ICT Information and Communication technology) including interactive Whiteboards, storage devices, personal digital entertainment devices (PDEs), MP3 players, personal digital assistants (PDAs), mobile phones, laptops, desktops, tablet PCs, gaming devices, assistive and adaptive technologies, digital cameras, scanners, smart cards and a range of content delivery methods.

The CSL supports and encourages the use of personal technology and is pleased that students have access outside of school. Use of personal devices, however, cannot be tolerated in schools or classrooms during school hours. Devices such as Smartphones, personal laptops, chromebooks, iPads and other tablets are not to be used in schools or classrooms unless special authorization has been granted and the device is properly monitored.

Should a student bring in a device and use it without authorization, he or she will be subject to the following progressive consequences:

- 1st offence: electronic item is taken away for the day and sent home at the end of the day with the student. The teacher notifies the parent and notes the date.

- 2nd offence: electronic item is taken away by the teacher. The parent is phoned by the teacher and the parent will be required to pick up the item from the school. Incident recorded by the teacher and dated.

- 3rd offence: electronic item taken away by the teacher. The student's privilege to bring the specific item to school is revoked. A letter will document that this is the third incident. The parent will be asked to pick up the item. At this point, the teaching environment, the student's learning (and/or the rights of others) is being compromised. The incident is noted and dated

N.B. If the situation is not resolved, the student risks suspension.