DIRECTIVE ON THE USE OF COMPUTER RESOURCES AND SOCIAL MEDIAS

Department responsible : General Administration	***Approved by :*** Director general
Effective date : January 1st 2003	***Amended :*** September 4, 2007, June 18, 2012, December 3, 2013, and June 6, 2018
References : CC 2011/2012-33 ADM-03 / Copyrights ADM-10 / Protection of personal information & Access to information EQU-01 / Purchasing art. 6.2	

1. PREMISES

1.1 purpose and application

Kativik Ilisarniliriniq recognizes the importance of access to its computer resources and telecommunications network by its students, employees and elected members. This directive sets the rules and procedures pertaining to the use of these resources in schools, Adult Education learning centers, administrative centers and any other facility under the jurisdiction of Kativik Ilisarniliriniq.

As owner and manager of its computer resources and telecommunications network, the Board must ensure that their use follows applicable laws and respects certain standards. The Board expects that its educational and administrative objectives will be respected during the use of these resources.

The Board also expects that each user will follow generally accepted rules of propriety and courtesy as well as applicable laws and regulations.

1.2 objectives

This Directive establishes conditions for the use of computer resources, and is intended to:

- promote responsible use of the computer resources;
- contribute to the educational mission of preparing students to become active members of society;
- maintain the School Board's reputation as a responsible educational organization;

- prevent abusive and illegal use of computer resources by users;
- ensure protection of personal information;
- define the limits of users' personal privacy when using computer resources;
- minimize the risks of system and data destruction or alteration.

1.3 legal framework This Directive was developed in conformity with the following legal framework :

- *Civil Code of Québec* (RLRQ, 1991, C-64);
- *Act respecting Access to documents held by public bodies and the Protection of personal information* (RLRQ, c. A-2.1);
- *Copyrights Act* (L.R.C., c. C-42);
- *Criminal Code* (L.R.C. 1985, c. C-46);
- *Charter of Human Rights and Freedoms* (RLRQ, c. C-12);
- Other relevant KI policies and directives in effect.

2. DEFINITIONS

2.1 definitions In this directive, the following words or expressions mean :

a) **administrator**: a school principal, a centre director, a director of an adult education centre, the director of student services for post-secondary students, the director or coordinator of a department or their delegate;

b) **computer resources**: without limiting the generality of this expression, all servers, computers, peripherals, storage, reception and data processing accessories and all software, information and data banks (of text, sound, graphics or other visuals) located in or on computer equipment or media, e-mail systems, or on a Web site, and all computer communications networks owned or leased by the School Board;

c) **educational centre**: a school, Adult Education learning centers or any other facilities used for pedagogical purposes;

d) **educational purposes**: use of the system for classroom activities, professional or career development and self-discovery activities. These may include academic exchanges, special projects, support services, curriculum and professional development activities;

e) **IT Department**: the department of Information and Technology of the School Board;

f) **social media**: social media is defined as all forms of online applications, platforms and virtual media that facilitate interaction, collaboration and content sharing and delivery. Social media on the Internet include, but is not limited to:

- Social networking sites (Facebook, My Space, Digg, Ning, Friendster, LinkedIn, etc.);
- Video or photo sharing sites (Facebook, Flicker, YouTube, ITunes, etc.);
- Micro "blogging" sites (Twitter, etc.);
- Personal or corporate blogs hosted by traditional media (Videotron, Canoe, Journal de Montréal, TVA, Radio-Canada, etc.);
- Discussion forums (Yahoo, Groups, Google Groups, Wave, MSN Messenger, etc.);
- Online encyclopaedias (Wikipedia, etc.);
- Any other website that allows users or companies to use online publishing tools.

g) **student:** a student in the youth sector, adult education or post-secondary sector;

h) **user:** elected members, employees, students and any other individual or organization called upon or authorized to use the computer resources.

3. GENERAL PRINCIPLES

3.1 privilege Access to computer resources does not constitute a right, but is a privilege. The use of this privilege must be reasonable and must not unduly limit other users' access to computer resources nor degrade network performance.

3.2 disclaimer All users having access to the Board's computer resources must acknowledge that the Board does not accept any responsibility for the use or misuse of information acquired, as for any situation, issue, litigation that may arise from unauthorized use or contravention to the rules set in this Directive.

3.3 priorities Computer resources are made available to users, as required by their duties, for learning, teaching, management and administrative activities and for community services related to the mission of the Board.

3.4 personal use Personal use of the Board's computer resources is allowed under certain conditions :

- it does not interfere with the work performance of the employee or of other employees;
- it does not interfere with the pedagogical activities of the student user or of any other students;
- the user is responsible, when applicable, for equipment usage and material fees;
- the user respects the stipulations described in the present Directive even when computer resources are used for personal reasons.

Users must accept that the Board has access to communications and transactions made using its computer resources, and therefore personal use cannot be considered private.

3.5 forbidden use The user shall not engage in any of the following activities, however this list should not be considered exhaustive:

a) using the network to create, download or distribute any image, sound, messages or other materials which are obscene, harassing, racist, inflammatory, malicious, fraudulent or libelous;

b) using the network for any activity that may be considered unethical or immoral;

c) using obscene language;

d) harassing, insulting or attacking others;

e) damaging computers, computer systems or computer networks;

f) violating copyright laws[1] and the duplication and distribution of software licensed to KI;

g) limit access to a computer by adding a password without authorization;

h) searching or otherwise collecting information about others with malicious intent;

[1] See Directive ADM-03 / Protection of Copyrights

i) gaining unauthorized access to folders, work, files or accounts;

j) employing the network for commercial purposes not related to Board activities except in the case of educational projects approved by the Director-General;

k) bandwidth usage at the detriment of other users (i.e. Youtube, Torrent, Skype, etc.);

l) duplicating, exchanging or using illegally acquired or malicious software;

m) using, taking materials, writings or images belonging to others and presenting them as if they were one's own (plagiarism);

n) spamming, i.e. sending unsolicited e-mails for purposes unrelated to the work, for example, personal advertising;

o) sending chain emails;

p) soliciting for or promoting religious or political causes;

q) downloading of games or entertainment programs, except for pedagogical purposes as authorized by the competent authority;

r) posting of personal information or images without the permission of the individual, the administrator or of the parents in the case of minors.

3.6 high jacking/ signal — It is forbidden for anyone to add a wireless device to a KI network without prior authorization of the IT Coordinator.

4. EXTRA-CURRICULAR ACTIVITIES

4.1 Internet outside regular class activities — It is the sole decision of each educational center to set up extra curricular activities involving access to Internet, depending on the available resources.

5. E-MAIL

5.1 respecting message confidentiality and integrity — Users must respect, when applicable, the confidentiality of messages delivered via the network, and are forbidden from intercepting, reading, altering, circulating or destroying messages intended for someone else.

5.2 forbidden actions

Users are strictly prohibited from :

- using deception or other means to transmit e-mails anonymously or under another name;
- subscribing to an e-mail lists having no relation to the user's duties;
- sending, without authorization, to all personnel or to groups of personnel messages on various subject not relevant to the activities of the School Board.

5.3 e-mail address - employees

Once an employee is provided with a KI address, he shall use this address for any internal or external communication related to his employment or duties. The KI email address will be the only email address used by the employer for any official email correspondence with the employee.

6. SOCIAL MEDIA

Social media is an integral part of modern life. It is a powerful communications tool that has a significant impact on organizational and professional reputations. Because it blurs the lines between personal voice and institutional voice, KI has defined the following rules and procedures to help clarify how best to enhance and protect the personal and professional reputation of its elected members, employees and that of KI when participating in social media.

6.1 accountability

Employees and elected members are accountable for anything they post on social media sites and they should never share information with elected members, students or other staff members that they would not share in a school or work environment.

Once information is posted on the internet, it will always remain available in the future.

6.2 identification during online communications

It is prohibited for employees and elected members to associate their personal remarks with the name of the School Board or with that of one of its institutions, or to suggest that the opinions they express are endorsed by the School Board or by the institution, except when this is done by a person authorized to do so in the performance of his or her duties.

Thus, when speaking on a subject that may affect KI, employees and elected members should post a disclaimer such as: "The comments posted on this site represent my personal opinion. They do not necessarily represent the position or opinion of KI ".

6.3 standards As a rule, employees and elected members need to follow the same behavioural standards online as they would in real life. The same laws, professional expectations, and guidelines for interacting with students, parents, media, and other KI constituents apply online as in the real world.

6.3.1 **Duty of loyalty**

Without limiting the generality of the foregoing, elected members and employees shall, both when using platforms administered by the School Board and personal accounts (e.g. Facebook, a blog, etc.) or other platforms :

- Refrain from disrespecting, threatening, intimidating, insulting or denigrating the School Board, its elected members, its employees or its students, or from disclosing false or defamatory information about them, or otherwise damaging the image and reputation of the latter.

6.3.2 **Role model for students**

The elected members of the School Board and the employees who work with students act as role models for them. This role is exercised both within and outside the School Board. Special attention must therefore be paid when using social media.

In this context, and without limiting the generality of the foregoing, when interacting with students through social media, they must maintain the necessary distance in order to respect their duty of professionalism, act as role models for students and avoid conflicts of interest.

6.4 respect for confidential information At all times, employees and elected members must protect the confidentiality of personal information about students and their families, employees and elected KI members.

In this context, and without limiting the generality of the foregoing, they shall :

- Obtain prior written authorization from the elected members, employees, members of the community or students of the School Board (or the holder of parental authority in the case of a minor) before publishing a photo, video or sound recording concerning them in the official publications of the School Board (paper, electronic, web and social media publications through the institutional accounts of the School Board and its schools).

The same rule applies when photos, videos or sound recordings were taken as part of school activities or activities organized by one of the School Board's establishments, and an employee or elected member wishes to publish them on a personal account (for example, Facebook, a blog, etc.);

This rule does not apply as regards public events that are not organized by the School Board.

6.5 worthwhile information

Employees and elected members should strive to add value and perspective by providing worthwhile information when participating in social media.

7. COPYRIGHTS AND SOFTWARE LICENSING

This section should be read in conjunction with the Directive ADM-03 on the Protection of Copyrights.

7.1 intellectual property on Internet

Intellectual ownership of the information on the Internet is considered to be in the public domain, for immediate direct access only. Specific requests for information and access are subject to copyright laws and site rules. Unless specifically acknowledged otherwise, the information accessed via the Internet is assumed to be the property of the site accessed, and cannot be distributed or modified without the express permission of the appropriate granting authority.

7.2 software protection

KI must respect the provisions of copyright laws in the area of computer programs and media. In an effort to discourage the violation of copyright laws and to prevent prohibited activities, the following rules are set :

a) only legal copies of programs that are licensed to the Board may be used on KI equipment;

b) no additional software or programs may be installed or downloaded on computers without the prior approval of the administrator.

7.3 intellectual property/ data

Data created by users remain the property of the Board as established by the Policy on Copyrights / ADM-03.

8. CONFIDENTIALITY AND PROTECTION OF PERSONAL INFORMATION

8.1 confidential information

Despite security precautions, there is no fail-safe measure to prevent an unauthorized individual from accessing stored files. The system administrators cannot guarantee the confidentiality of electronic correspondence. It shall be the responsibility of the users sending confidential information to ensure that there is an appropriate level of security measures in place.

USER OBLIGATIONS

8.2 respecting protective mechanisms

Users must conform to the Act respecting Access to documents held by public bodies and the Protection of personal information (R.S.Q., c. A-2.1) regarding the conservation, access, transmission and distribution of information through use of computer resources[2].

8.3 publishing personal information

Users may not publish, without permission of the individual, personal information in the form, text, photograph or any other type of content.

Student users must be informed of the appropriate on-line behaviour when transmitting personal information about themselves, their family, friends or any other person.

9. CREATION OF WEB PAGES

9.1 school board web pages and institutional social media accounts

Schools and departments may, with the assistance of the KI webmaster, establish their own web pages within the KI web site that present information about the school or department activities. The departments are responsible for maintaining the content of their web pages.

The School Board's corporate social media accounts on social networks are managed by the communications team and content is developed in collaboration with the departments and schools where applicable.

Schools can, with the help of the KI webmaster, create their own website. Schools are responsible for maintaining the content of their websites. Schools can, with the help of the communications team, create and manage their own corporate school account on social media. Where a corporate school account already exists, it is this account that must be used.

---

[2] See Directive *ADM-10 / Protection of Personal Information & Access to Information*

9.2 links to other web sites and/or advertisement

Links created within a school web page or a student personal web page may not be for commercial purposes or advertisement without specific authorization from the Director-General. Outside organizations may not link to a school web page for their own benefit to advertise a product or event of a commercial, political or religious nature.

10. EMERGENCY AND SECURITY MEASURES

10.1 verification

The School Board reserves the right to maintain a registry of on line access made through use of its computer resources and telecommunications network and the right to analyze information contained in the registry in order to detect unauthorized, illicit or illegal activities on its network.

The Director General may authorize that verifications deemed necessary are done and that copies of documents, data or information are kept when there is a serious doubt that this Directive as well as other directives issued by the School Board that ensure the application of relevant School Board agreements and protocols or provincial and federal laws and regulations are not respected.

The IT Department may proceed with required verification, when an emergency situation justifies it, such as the detection of a virus in the network or overuse of the network's resources threatening the integrity of the network.

The School Board reserves the right to remove from its computer resources any content that is illegal or that contravenes the present Directive.

10.2 suspension of access rights during verification

A user's access rights may be suspended during verification. Such a decision is the responsibility of the user's immediate supervisor in the case of employees and the school principal in the case of students.

10.3 security

The IT Department implements computer tools that ensure :

- the security of the computer resources;
- protection against viruses, intrusions or alterations of data;
- prevention of illicit usage.

The IT Department Coordinator can develop rules to ensure the security of the computer resources and proceed with periodic security audits.

10.4 password Users who install "user level" passwords to secure a computer or software must provide this password to their immediate supervisor. In the case of schools general use computers, the password must also be provided to the IT Department.

In the case of general use computers in the schools, users are prohibited from modifying "Administrative level" passwords on their computers.

Users working with confidential information stored on their computer shall always maintain "user level" password security.

10.5 anti-virus It is forbidden to disable any anti-virus or system stability software installed by the Board.

10.6 mandatory backup Users are expected to take the necessary measures to safeguard the data they created in the course of their work by implementing a sound backup method.

10.7 digital signature The school board recognizes the validity of an electronic signature for approval of administrative forms when the following constraints are respected :

a) the employee signing the form has the authority to do so;

b) the signature is associated with a specific employee in the system;

c) a personal identification number (PIN) is used to validate the application of the signature to the form as required by the system.

Each employee is responsible for keeping the PIN associated with their electronic signature private.

11. SANCTIONS FOR VIOLATIONS

11.1 consequences for inappropriate use Any violation by a user of any provision set in this Directive will result in disciplinary action such as:

a) suspension or removal of access to computer resources;

b) appropriate measures as determined by the appropriate level of authority, including dismissal;

c) appropriate legal action including criminal prosecution, when applicable.

11.2 investigations When an investigation is required, it is done under the authority of the Director General and the Associate Secretary General.

12. APPLICATION OF THIS DIRECTIVE

12.1 previous provisions The present Directive replaces all other directives of the Board pertaining to this subject, while respecting the policies adopted by the Council of Commissioners where applicable. If such policies are adopted, the provisions of these policies will be integrated into this directive for the benefit of the reader.

12.2 responsibility Any person referred to in this Directive must abide by all its provisions and all managers of the School Board are responsible to ensure that all its provisions are applied and respected.

The Associate Secretary General is the person responsible for providing support in the interpretation of this Directive and to ensure its revision when necessary.