INFORMATION HIGHWAY, CAUTION SCHOOL ZONE

In 1996-1997, the Ministère de l'Éducation du Québec (MEQ) invited Quebec schools to plan the introduction of new information technologies over a five-year period.

The first step was to purchase equipment and teaching materials. The plan included Internet connection to initiate students to the most commonly used functions such as browsing, creating Web pages, and electronic mail. Other applications are also accessible like discussions with students from the same school, the same region, or even from other countries, in deferred or direct mode. In the course of their educational activities, some schools have displayed on their Web sites information about their students to make them or their interests better known. An Internet Web site is the equivalent of a public square. The information carried on international networks passes through many unidentified operators and countries where personal information generally is not regulated.

In this context, Internet raises concerns about the privacy of users, who, in the course of their activities, may communicate personal information without knowing how it is going to be used by the organisation or the person accessing it.

The proliferation of school Web sites and the use of other Internet functions have prompted the Commission d'accès à l'information to caution school boards and private teaching institutions, schools, their staff, and other educators, and suggest ways of ensuring the protection of personal information and, more broadly, the privacy of students in the educational environment.

The goal is to tailor the use of new technologies to the school boards' obligation to respect the privacy of students.

We must bear in mind that in any information system, there is a direct link between the degree of security and confidentiality and the protection of personal information. Effective protection calls for a series of measures to ensure the security of data stored by an organisation. The introduction of any new technology provides an excellent opportunity to study its impact and detect potential areas of vulnerability. Physical and logical security, in particular, should be examined. The Commission encourages such efforts to strengthen the protection of personal information.

Whatever measures are put into place, however, we should be reminded that awareness, education, and the commitment of all those involved remain the best guarantee of privacy.

This document is the result of the work of a committee formed by the Commission and made up of representatives from a number of organisations. It has been prepared in a way that takes into account the roles and responsibilities of the various members of the educational community. The following cards contain information intended for school boards, private teaching establishments, school principals and staff, and students and parents to help them protect their privacy while surfing on the net.

SCHOOL BOARDS AND PRIVATE TEACHING INSTITUTIONS

School boards and private teaching institutions governed by the *Act respecting Access to documents held by public bodies and the Protection of personal information* (Access Act) and private teaching institutions governed by the *Act respecting the protection of personal information in the private sector* (Private Sector Act) must ensure that when Internet is used in school for educational purposes, the students' personal information is protected.

Let us recall that under the law**, personal information is information that concerns and can identify a physical person**.

The Access Act and the Private Sector Act compel school boards and private teaching institutions to ensure the confidentiality of student data in their possession. Except in specific cases, no personal information can be divulged without the consent of the person concerned. If the person is a minor, the person holding parental authority may give consent.

Therefore, a student's personal data cannot be displayed on a school's Web site or used in other Internet functions without the parents' consent.

To help school boards discharge their obligations, the Commission proposes measures to protect personal information when creating or developing a Web site, or using other Internet functions.

Standards for the creation of Web sites and the use of Internet by students

School boards and private teaching institutions, in cooperation with parents and their teaching and professional staffs, should establish rules for the display of students' personal data on their Web sites.

Taking into account the issues raised by the students' use of Internet, standards or a code of ethics should also govern the attribution of an electronic address, the use of electronic mail, participation in discussion groups or Internet relay chats, students' supervision, the role of the various participants, and the information to be provided to parents.

The absence of standards can lead to different, contradictory policies within a school or from one public school to another.

Appointment of a resource person

The appointment of a resource person to coordinate the protection of personal information when developing a Web site would help standardise the information circulating within a school board or a private teaching institution, especially for the display of personal information on the Web sites of public or private schools, the students' use of other Internet functions such as electronic mail, and the responsibilities of the different contributors.

**Information on plans to create or develop
a school Web site**

To ensure the protection of personal information, school boards or private teaching institutions should keep track of the development of Web sites and require to be informed of any such project in public or private schools.

Thus, the school board or private teaching institution will be in a position to verify that the sites meet the established standards.

THE SCHOOL

Public and private schools are responsible for the supervision and the security of students during school hours. They must, in some circumstances, inform parents of organised activities and ask them to authorise their child's participation. During such activities, personnel or volunteer parents are assigned to supervise the students and ensure their security.

Browsing the Internet is an activity that may threaten the privacy and the security of students. We caution children against speaking to strangers on the street. The same logic should apply when a student browses the net and links with strangers, particularly through electronic mail. The school, therefore, should take steps to enable students to navigate safely.

Appointment of a coordinator for the development of a school Web site and the use of Internet

To ensure a coherent application of the standards set by the school board or the private teaching institution for the protection of personal information, a representative should be appointed by the school to coordinate a school's Web site development. This person, in cooperation with the school, parents and the personnel concerned (teacher, professional or other), could apply the standards for the circulation of personal information and the use of Internet by students, including electronic mail and discussion groups or relay chats.

Internet access provider

The school should deal with an access provider who can guarantee the safety of personal information. The service agreement should include a commitment by the server to ensure the confidentiality of the students' personal information he stores and not to use such data for purposes other than those specified in the contract. Likewise, provisions should guarantee the destruction of personal information once the provider no longer requires it.

A student's electronic address should be such as to make it impossible to identify or trace the student without his consent or that of his parents.

An electronic address including the student's name and surname, for instance, becomes nominative information.

Supervising the use of Internet in school

The planetary scope of Internet and the absence of international legislation governing the content of sites and the circulation of information make it difficult to control sites that contain violent or pornographic material. The same is true of discussion and chat groups, which are not censored.

To prevent them from accessing sites or discussion groups that might threaten the safety of their personal information, students using Internet functions as part of their curriculum need to be supervised.

The appointed staff (teacher, professional or other) must keep a close watch over the students' use of electronic mail to prevent them from sending or receiving malicious or hate messages. They should inform students that they can overlook at all times, like any other school work, the electronic mail they send or receive in the course of their school activities.

They should also advise students to inform their professor at once whenever they receive a suspicious message.

A students' code of ethics

To raise student awareness about the circulation or use of personal information on Internet, the school should consider having them sign a code of ethics.

For participation in discussion or chat groups or electronic mail, for instance, the code should require students to avoid communicating personal information about themselves or others without first verifying their correspondent's identity. In case of doubt, they should avoid identifying themselves.

Students should also undertake to refrain from circulating untruthful, hateful or malicious information about third parties or other students.

Parent information

The school should inform parents of Internet activities involving the use of personal information about students.

To enable parents to fully understand the issues raised by their child's use of Internet, it would be important that the school tell parents about the precautions taken to ensure the protection of personal information. Thus, parents could give informed consent to their child's participation in such activities and authorise the circulation of personal information, particularly through electronic mail.

A regular check of documents displayed on Internet

Needless to say, when school works are displayed on the school site, the teaching staff or the person appointed for this purpose should ensure that the information or the documents prepared by students are in keeping with the standards set by the school board for the protection of personal information.

THE TEACHING AND PROFESSIONAL STAFF

During school hours, the teaching and professional staff is responsible for educating the student and ensuring his safety. As any good parent should do at home, the teacher must be vigilant when students browse the net.

Information on issues raised by the use of Internet

In the course of educational activities involving the use of Internet, the teaching staff should make students aware of threats to their privacy and that of their parents whenever they browse the net or circulate personal information.

For information purposes, the teaching and professional staff could draw inspiration from the instructions contained in the information sheets intended for primary and secondary school students in this document.

The supervision of Internet activities

There should be a regular check of documents displayed on the school's Web site to ensure that their content is in keeping with the standards set by the school board for the circulation of personal information on the site.

To primary school pupils

To navigate safely on Internet or design a risk-free site, here are some cyberrules you should observe:

Personal information

- As part of an educational activity on Internet, ask your teacher before giving out personal information. For example, your name, your picture, your telephone number, your home address, your electronic address, your age, your favourite activities, the name of your school, the address and telephone number of your parents at work …
Even if you're asked by your favourite cartoon character, if you're offered gifts or if it is a condition of access to a site, a club or a game, it is unwise to fill out forms.
When you leave a message in a discussion group or join a chat room, other people may see what you are entering. Do not give out personal information.

Strangers

- You know how to be careful and beware of strangers in real life. Remember to do the same on Internet. If you are unsure of your correspondent's identity, you should not identify yourself.

- It is dangerous to agree to meet a cyberfriend you got to know on Internet. If you are really eager to meet someone you chatted with on Internet, do so in a public place and accompanied by a parent. You cannot see the people you chat with on Internet: they might turn out to be different from what you imagine.

Messages

- No one should ever send insulting or aggressive messages. You should not reveal personal information about other people either.

- If you find a message suspicious, don't answer it. Disconnect and inform an adult immediately.

- Everything you say or do on Internet does not necessarily remain confidential.

Browsing the Internet

- When you choose a password, make sure to choose one that is difficult to guess, but that you will remember. A password is secret and should not be revealed to anyone.

- It is wise to discuss with your parents what use of Internet is permitted.

- If you find sites where they try to sell you things, beware; don't accept any offer without your parents' authorisation.

- Don't believe everything you read on Internet. Check the source of information and have a parent or a teacher confirm the information.

…. If you have doubts… speak to a parent or a teacher.

To secondary school students

What's interesting on Internet is interactivity. Making new friends all over the world is exciting. However, caution should be exercised when browsing the net. Here are a few tips to navigate safely:

Personal information
- It is unwise to give out personal information on Internet (your name, your address, your age, your interests, your picture…). If you are required to do so on a commercial site, be sure to check the identity of the organisation operating the site (take down the name, location and telephone number). Check whether the site has a privacy policy, and give only the information required for the purpose of your request. Any communication should be considered unsecured unless a safety mechanism is activated. For example, the browser displays a complete key at the bottom of the screen when the message sent is coded (the plain text is replaced by a text unreadable to anyone who does not have the key to restore it to its original form).

Strangers
- If you are not sure of your Internet correspondent's identity, it is preferable not to identify yourself. Do not give any information about yourself or a third party in discussion groups and chat rooms. Always bear in mind that your chat mates may not be who they claim to be.

- It is risky to agree to meet a friend you got to know on Internet. If you are really eager to meet a person, do so in a public place and accompanied.

Messages
- It is wise not to answer insulting or aggressive messages or a stranger's questions that make you uncomfortable. Save the message and, if you feel it is necessary, show it to the person in charge at your school.

- Hate messages should never be sent out on Internet.

- Electronic mail is not entirely safe. What you write may not remain confidential.

Surfing on Internet

- Beware of purchases on Internet and offers that are too good to be true.

- Not everything you read about Internet is true. You would do well to check the information sources.

- A password should be difficult to guess and should not be revealed to anyone (even to your access provider). Change your password regularly and configure your electronic mail so that it does not log your password.

- Your use of Internet leaves trails…Inquire from your Internet access provider what use is made of the information concerning your use of Internet and how secure it is.

To parents

The Internet is an unprecedented means of communication, and one that occupies an ever-larger place in the lives of our children.

The activities children find most attractive are undoubtedly those that allow them to communicate directly with their peers, for example discussion groups, chat rooms, or electronic mail.

We should be aware that this new technology offers global communications and is accessible to all. A prudent child can navigate on Internet as safely as he can walk in a park, a shopping mall or another public place.

The gathering of personal information

Most Internet sites do not ask personal information of those who visit them. However, such is not the case for commercial sites.

Children make up a large proportion of Internet consumers and their number increases rapidly. They are a highly valued target of commercial sites.

Many commercial Web sites seek to collect personal information from young people. They do so through membership forms for games, clubs, questions directed at the child, the signing of guest books. They often make it a condition of admission to the site or to a contest offering prizes. They might also seek the information through a cartoon character or a personality known to the child. A U.S. study released last June[1] surveyed 188 commercial sites that collect personal information from children; it reported that 96 % of these sites collect the electronic mail address, 74 % the name of the child, 49 % his home address, 46 % his age or his birth date.

Therefore, it is important that children be careful when they are asked [23]personal information.

Web exchanges

Discussion groups are very popular among young people. The topics discussed are not subject to any control and the identity of the persons with whom the cybernaut agrees to chat is unknown.

Either through discussion groups, chat rooms or electronic mail, children may receive aggressive messages that they may find threatening.

---

[1] Privacy Online : A report to congress, Federal Trade Commission, U.S.A., June 1998

The most serious threat to our children is no doubt the communication of personal information that makes it possible to identify the child in a public interactive area such as a discussion group or a chat room accessible to all connected cybernauts. Children can communicate freely with strangers, including adults. The persons with whom your child communicates can easily conceal their identity. The "13-year old girl" may well be a 45-year old man. FBI investigations have shown that on-line services have rapidly become the most valuable resource of predators, enabling them to identify and contact children. Traditionally, parents caution children against talking to strangers. Children receive the opposite message when they are encouraged to communicate on-line with strangers through the Web.

Therefore, children should not give personal information about themselves or their families on the Internet when they are not sure of their correspondent's identity.

Here are a few simple rules to teach your child:

Personal information

- Unless they are in a safe environment or they know their correspondents, children should refrain from offering personal information (name, birthday, address, telephone number, the school they go to, personal or family photographs, etc.). Talk to your child about privacy on the Web. Make sure he understands why he should not offer personal information on the Web.

Strangers

- If your child is unsure of his correspondent's identity, he should not identify himself.

- It is unwise for a child to meet with someone he got to know on Internet. If your child agrees to such a meeting, make sure the meeting takes place in public and in your presence.

Messages
- Children should not reply to threatening or obscene messages. If your child feels threatened by questions asked by a stranger, he should save the message and inform you. If need be, you should inform your Internet access provider.

Browsing the Internet

- Caution your child against commercial sites and agreeing to anything without your permission.

- On the Internet, anybody can become an information provider. It is important that your child develop critical judgement about the information found on Internet.

- If your child has a password to access Internet, make sure he does not reveal it to anybody (even if the Internet access provider asks it). Hackers may use your account and you may be faced with unforeseen charges on your bill.

- Consult privacy policies of the sites you visit with your child and especially those where you leave information about you. Your visits may leave trails.

Parental supervision

- It is wise to inform your child of the rules to observe for safe browsing on the net. Stick around while your child is on-line. Children quickly learn how to use computers, but their limited life experience may lead them to divulge information you do not want to be shared. This is why your child should be supervised when he ventures into cyberspace. Check the sites he visits and explain to him why he should not identify himself in discussion groups, chat rooms and on-line correspondence. Technologies are available to restrict the use of Internet. For example, "access control filters" can prevent your child from accessing certain documents or sites and/or discussion groups that are inappropriate for a person his age. However, these tools are not foolproof. Parental commitment, participation and supervision are essential. Awareness, education and parental commitment remain the best tools of privacy protection.

Internet access provider

- Subscribe to a responsible Internet service provider. Enquire about your Internet provider's confidentiality policy, his practices regarding the personal information he stores about you, and the security surrounding the trails that are left from your Web use.

- If you don't want to be identified by your electronic address, choose one that does not include personal information. If you don't want to receive advertising mail, make sure as best you can that your name and the names of members of your family are not included on any list (electronic directories of electronic addresses, for example)

GLOSSARY

Definitions of Internet services used in schools
from the standpoint of personal information

Internet is a global computer network offering a host of services to users: the two most popular functions are Web sites and electronic mail. Other services are quickly gaining in popularity. Discussion groups, distribution lists, and direct chat rooms are particularly favoured by 12 to 20-year olds. There are also more specialised services to access remote servers, transfer files, etc., but they are less used in the school environment.

Here is a list of the main services available on Internet. The boxes provide concrete examples of their use.

Internet or Internet network:

The Internet is a collection of thousands of computer networks, tens of thousands of computers and millions of users who share a compatible means for interacting with one another to exchange digital data. It is made up of national, regional and private computer networks linked by the TCP-IP communication protocol and cooperating to offer a single interface to users.

Web or W3 (World Wide Web, WWW):

A hypertext-based system that allows browsing of available Internet resources.

- *Browsing the Web*: Visiting a library, museum, store, family, country, etc. Browsing the Web is like paying a visit to the so-called "virtual" world.

Web Site:

Internet site storing data accessible on the Web.

- *Create a Web site*: Displaying one's work, class, etc. A Web site allows the storage of texts, images and sounds created by students and makes them accessible to everybody browsing the Internet.

Electronic mail (e-mail)

An electronic message delivered from one computer to another.

> • *Electronic mail*: Message to a friend, relative or correspondent addressed to one or more persons selected by the sender. Generally, the sender knows to whom he sends the message and can receive replies from the persons contacted.

Forum, discussion forum, discussion group:

Service offered by an information provider or an electronic bulletin board on a network like the Internet enabling a group of individuals to exchange opinions, ideas on a particular subject, either directly or in deferred mode, according to various formulas (list of participants, IRC channel, etc.)

Note: Now that most bulletin boards and mail services are linked to the Internet, these terms (discussion group, news group, forum, etc.) are used as synonyms to describe the service, the group itself and the virtual location of the meetings.

> • *Discussion groups*: Reading and writing texts on a given topic to exchange opinions and ideas with strangers sharing common interests. The writer does not know whom he is addressing, except in restricted private discussion groups.

Chat, cyberchat:

Real-time interactive character-based communications available to Internet users with interactive access.

> • *Chatting*: Talking through the keyboard with strangers whose identity is concealed. Participants identify themselves only by a nickname and often create an imaginary character. Thus, a person's description may be fictitious.