Commission scolaire English-Montréal English Montreal School Board		
POLICY:	**INFORMATION AND COMMUNICATION TECHNOLOGIES – ACCESS AND APPROPRIATE USE**	**CODE: DG-25**
Origin:	Technology Access and Security Committee (TASC)	
Authority:	Resolution #11-11-23-12.2	
Reference(s):	Previously Code: PS-14	

POLICY STATEMENT

In support of its commitment to promote and support the use of Information & Communication Technologies (ICT) in the learning and teaching process, the English Montreal School Board (EMSB) undertakes to:

- Ensure the provision of appropriate resources in a fiscally responsible manner;
- Establish mechanisms, policies, and procedures to safeguard user rights and to ensure that its ICT services and resources are used in a responsible way;
- Hold all stakeholders responsible for the appropriate use of EMSB ICT Systems;
- Continuously sensitise all stakeholders to the appropriate and secure use of ICT;
- Restrict access to Internet sites with appropriate content as identified in Appendix VII – Internet Filtering.

FIELD OF APPLICATION

This *EMSB ICT Access and Appropriate Use* policy, hereafter known as the "Policy", applies to the telecommunication and computing infrastructure, equipment and services provided or managed by the EMSB, or any external systems accessed while using these services, including any software installed or running within EMSB-managed systems. Additionally, this applies to any ICT which may presently, or in the future, be provided through other sources for use at the EMSB either directly or remotely.

The Policy also applies to all ICT stakeholders (employees, students, Commissioners, parents, general public, etc.) that access or use EMSB ICT.

PURPOSE

The EMSB recognises the importance of ICT in the learning and teaching process.

The purpose of this policy is to:

- Promote the secure and appropriate use of ICT throughout the spectrum of EMSB administrative and educational activities;
- Define the respective responsibilities of all EMSB ICT stakeholders with respect to the effective, appropriate, legal, ethical, educational, and employment related use of ICT;
- Respect the privacy of personal and organisational information.

PRIVACY AND PROPRIETY RIGHTS

1) The EMSB extends the privilege of reasonable personal use of the EMSB's ICT Systems to all employees;

2) The EMSB has the right to monitor and log all accesses and use of all its ICT Systems, including but not limited to the monitoring of Internet site accesses, downloaded files, and email systems.

   Therefore, since the privilege of reasonable use of EMSB's ICT Systems is extended to its employees, the EMSB shall act discreetly and in a confidential manner in the event that an investigation of possible inappropriate use is required;

3) Employees and students should have no reasonable expectation of privacy when using EMSB's ICT Systems;

4) Employees should be aware that any work created or stored on EMSB ICT Systems, whether or not related to their job function, remains the property of the EMSB the whole in compliance with the Copyright Act (R.S.C., 1985, c. c-42);

5) Students should be aware that any work created or stored on EMSB ICT Systems remains the property of the student unless there is a prior agreement to the contrary with the EMSB.

EQUIPMENT, SOFTWARE, AND SERVICE REQUESTS

All purchases and installations of ICT Equipment, Infrastructure or Software are to be undertaken, coordinated or otherwise authorised by Information Technology Services (ITS) in conjunction with, in some cases, Pedagogical Services (PSD), Adult Education and Vocational Services (AEVS) or School and Centre Principals.

Equipment

1) Purchases of ICT Equipment must be processed through ITS via an email request to ITSupport@emsb.qc.ca, or through the EMSB Intranet site using the

"Computer and AV Equipment Request" system with a minimum of ten (10) business days notice;

2) Installation or configuration of new or existing ICT Equipment must be processed through ITS via an email request to ITSupport@emsb.qc.ca with a minimum of ten (10) business days notice;

3) Cabling additions or modifications for ICT Equipment must be processed through ITS via an email request to ITSupport@emsb.qc.ca with a minimum of ten (10) business days notice.

Software

1) Purchases of software, either administrative or educational in nature, must be processed through ITS via an email request to ITSupport@emsb.qc.ca, or through the EMSB Intranet site using the "Computer and AV Equipment Request" system with a minimum of ten (10) business days notice;

2) New software, not listed on either http://logicielseducatifs.qc.ca/ or the PSD Edu-Portal, that is educational in nature or intended to be used in a classroom setting must be approved by either PSD or AEVS prior to being purchased. The request may be sent via email to ITS for processing at ITSupport@emsb.qc.ca. Timelines will vary depending on the complexity of the software being evaluated;

3) Installation or configuration of software must be processed through ITS via an email request submitted to ITSupport@emsb.qc.ca with a minimum of ten (10) business days notice.

ROLES AND RESPONSIBILITIES

All ICT Stakeholders

All the ICT stakeholders must:

1) Adhere to and agree with the Policy by either formal signature or through electronic acceptance;

2) Refrain from using anonymous Internet services;

3) Refrain from creating, accessing, storing, sending, distributing or printing any material which is generally considered to be obscene, pornographic, erotic, sexually explicit, racist, abusive, discriminatory, hate-motivated, harassing, threatening, demeaning or otherwise objectionable in imagery or language;

4) Take reasonable precautions to prevent unauthorised access to EMSB ICT Systems. Such precautions include keeping login identifiers and passwords

confidential, and locking or preventing unauthorised access to your computer when left unattended for extended periods of time;

5) Refrain from storing personal files on EMSB equipment;

6) Copy files to central network storage to ensure the data is backed up. ITS provides data recovery services only for work-related files stored on network storage;

7) Report to ITSecurity@emsb.qc.ca any material received or stored in any manner (text, images, sound, etc.) which appears to be in violation of the Policy;

8) Respect and protect personal and confidential information regarding themselves and others;

9) Refrain from harming, attempting to harm, or destroying EMSB data;

10) Refrain from obtaining, by any means, access to any system, service, privilege or electronic material to which they are not authorised;

11) Refrain from violating Canadian copyright laws;

12) Refrain from installing unauthorised software on EMSB-managed computers;

13) Refrain from using Peer-to-Peer Services (P2P) or any evolution thereof;

14) Respect all laws and policies which specify appropriate use of computers and other telecommunications equipment;

15) Refrain from using EMSB ICT Systems, for personal monetary gain. This includes but is not limited to the solicitation of funds, advertising and selling of goods or services of any type unless such an activity is sanctioned by the School Board as represented by Director of the service or department of the employee;

16) Request permission from School or Centre Principals or consult the School Board Marketing and Communications Officer, as applicable, before releasing information that may appear to be sanctioned by the EMSB or is linked to official EMSB web sites;

17) Refrain from transmitting unsolicited bulk information (SPAM), including junk mail, advertising, jokes, solicitation, chain letters, virus alerts, etc.;

18) Ensure that non-EMSB devices are connected to the private EMSB network at any of its facilities only after authorisation, by making a request via email to ITSecurity@emsb.qc.ca at least five (5) business days prior to the required date.

Schools and Centres

It is the responsibility of the School or Centre to ensure that:

1) The purposes, benefits, and possible risks associated with the use of Internet resources are clearly communicated to students, parents, or guardians prior to access being provided;

2) Email accounts are distributed only to those students or their respective guardians that have reviewed and signed the Policy;

3) Activities related to ICT usage are planned, supervised, and implemented on the basis of their educational value;

4) ICT resources, including Internet sites, are previewed and evaluated for pertinence to the curriculum and learning needs prior to being recommended for student use;

5) Students are provided with clear directives for Internet access regarding compliance with school and centre guidelines;

6) Use of EMSB ICT Systems is supervised by EMSB employees or those authorised by the school to supervise the users.

Students

It is the responsibility of the student to:

1) Submit a signed Consent or Agreement Form (Appendix III, IV or V*)* signed by the student, parent or guardian, indicating agreement with the terms of provision of student access;

2) Use ICT Systems only with the permission and/or supervision of authorised EMSB personnel;

3) Immediately report to the teacher, supervisors, Vice-Principal, or Principal, any information, message or web site that is inappropriate or makes them feel uncomfortable;

4) Obtain permission from the supervising teacher or educator before printing.

PROTECTION OF CONFIDENTIAL, PROPRIETARY AND PERSONAL INFORMATION

Unless authorised to do so, employees or third parties working on behalf of the EMSB are prohibited from transmitting confidential or nominative information through any electronic medium to any party. Employees or third parties working on behalf of the

EMSB may not access, send, receive, solicit, print or copy confidential or proprietary information regarding the organisation, employees, suppliers, students, or other associates unless so designated by virtue of their job description or authorised to do so by their employer, or under the Act Respecting Access to Documents Held by Public Bodies.

Confidential information, includes, but is not limited to, employee or student lists, employee performance reviews, salary details, social insurance numbers, passwords, contact information and anything else that could cause harm to the EMSB, its employees or students were it to be made public.

Users are to respect the privacy of others and refrain from intercepting private communications and emails. The content of emails must not be altered for the purpose of falsification or distortion. Users must not forward information which the originator would reasonably expect to be kept private.

LIABILITY

The EMSB is not responsible for any loss or damage to users' data or storage devices, nor for any other problems incurred as a result of using its ICT Systems.

ENFORCEMENT

Instances of probable inappropriate use may be investigated. The EMSB shall act discreetly and in a confidential manner in conducting such investigations.

Investigations that uncover inappropriate use may result in the EMSB:

1) cancelling or limiting access to facilities or ICT Systems;

2) disclosing information found during the investigation to EMSB authorities, or law enforcement agencies;

3) taking disciplinary measures, including possible dismissal, according to collective agreement procedures, applicable laws and/or Schools' or Centres' behaviour codes.

A user will be responsible for damages to EMSB software and/or equipment resulting from gross negligence or intentional actions.

In those instances of probable inappropriate use by a Commissioner, the matter shall be referred by the Director General to the Governance and Ethics Committee. The Governance and Ethics Committee shall study the matter and make any recommendation deemed appropriate to the Council of Commissioners, including referring the matter to the Ethics Commissioner.

SYSTEM ACCESS MANAGEMENT

All EMSB systems must have appropriate user IDs and passwords to ensure access is restricted only to authorised individuals. Access authorisation is to follow the process identified in related Procedure Statements.

Passwords for all Users Except Elementary School Students

Passwords are used for various purposes such as: application accounts, web accounts, email accounts, screen saver protection, voicemail access and others. They must be treated as sensitive, confidential EMSB information. The EMSB requires that wherever possible, strong passwords must be used (see below for examples). This will significantly reduce security breaches of EMSB ICT Systems and improve the overall integrity and confidentiality of EMSB data.

For systems that allow users to change their passwords, all EMSB employees are required to change their passwords every ninety (90) days. The system will track a maximum of five (5) old passwords (i.e. you may use your first password only on the sixth password change).

Poor or weak passwords have the following characteristics:

- Contain less than eight (8) characters;
- Are common usage words such as: words found in a dictionary, company name, family names, birth dates, fantasy characters, word/number patterns such as; aaabbb or 12345, etc..

Strong passwords have the following characteristics:

- Contain more than eight (8) characters;
- Comprise a combination upper and lower case characters, digits and punctuation characters !@#$%^&*()_+|~-=\`{}[]:";'<>?,./.

  An example of a strong password is: *Ohmy1stubbedmyt0e!@#$%^&*

It is recommended that all EMSB users follow these best practice guidelines:

- Do not reveal your password to ANYONE. Do not reveal a password to co-workers while you may be on vacation. ITS will never request your password;
- If someone demands your password, refer them to this document or have them call the Director of ITS;
- Do not use the ”Remember Password” feature of applications or web sites;
- Do not write passwords down and store them anywhere in your office.

Passwords – Elementary Students

Passwords for elementary school students will be comprised of only alphabetic characters and no more than four in length. The students will also not be required or permitted to change their password during the school year.

Each student's password will be reset to a new value, by ITS, at the start of the school year prior to being distributed to the students' teachers through GPI.

NETWORK CONNECTIVITY

The EMSB network consists of two independent environments, each providing different services – specifically, a private network and a guest network. These networks are available either through a wired or wireless connection.

The private network has a higher level of security; it is managed and monitored on a regular basis to ensure availability, performance, and confidentiality of data. Access to this network at any EMSB facility is restricted to EMSB-managed devices or those that have been authorised by the Director of ITS. This is to ensure the overall security of EMSB systems and data.

Should it be necessary to connect non-EMSB devices to the private network at any EMSB facility, an email request outlining the justification for connectivity is to be sent to ITSecurity@emsb.qc.ca. Personal equipment connected to the EMSB private network will be subject to the same rules as EMSB equipment.

The guest network runs parallel to the private network and is meant to primarily provide Internet access to non-EMSB employees or connectivity for non-EMSB computers. Minimal security is established, and users are responsible for maintaining their system security such as anti-virus, spam filters, etc. In addition, there is no guarantee of availability or performance.

INTERNET USAGE

The EMSB provides employees and students with access to the Internet for activities and communications that support and relate to the mission, vision and strategic plan of the EMSB. Any user who violates these rules and policies is subject to disciplinary action.

Appendix VI documents Internet elements and how the EMSB will filter each one.

Authorised Personal Use of EMSB Internet Access – Employees

Employees may access Internet resources for personal use during non-work hours. Employees are prohibited from using EMSB Internet access to operate a business,

conduct an external job search, solicit money for personal gain, campaign for political causes or candidates, or promote or solicit funds for religious or other personal causes.

Authorised Personal Use of EMSB Internet Access – Students

Students may access Internet resources for personal use under the terms determined by the School or Centre. Students are prohibited from using EMSB Internet access to operate a business, conduct an external job search, solicit money for personal gain, campaign for political causes or candidates, or promote or solicit funds for religious or other personal causes.

Internet Privacy

Access to the Internet is provided by the EMSB and, as such, the EMSB has the legal right to monitor usage of the service. Employees and students should have no reasonable expectation of privacy when accessing the Internet from within the EMSB.

EMAIL USAGE

The EMSB provides employees and students with electronic communications tools, including an EMSB email system. This policy applies to the on-site or remote access and use of the EMSB email system. The EMSB email rules and policies apply to all users who have an EMSB email address. Any user who violates these rules and policies is subject to disciplinary action.

The EMSB allows email access for activities and communications that support and relate to the mission, vision and strategic plan of the EMSB. Employees may use the organisation's email system for personal use only in accordance with this policy.

For email best practices guidelines see the Email User Guide (Appendix IX).

Authorised Personal Use of Email

Employees may use email, either EMSB or their own Internet email (Yahoo, Hotmail, etc.) for personal use during non-working hours only.

Email Privacy

The email system is the property of the EMSB and, as such, the EMSB has the legal right to monitor usage of the system. Employees and students have no reasonable expectation of privacy when using the EMSB's email system.

Inappropriate Use of Email

Employees and Students are prohibited from using EMSB email to operate a business, conduct an external job search, solicit money for personal gain, campaign for political causes or candidates, or promote or solicit funds for religious or other personal causes.

Employees and Students are prohibited from using EMSB email to engage in activities or transmit content (text, sound or images) that is harassing, discriminatory, threatening, obscene, defamatory, or is objectionable or offensive according to Canadian and Quebec laws.

SOCIAL MEDIA USAGE

Existing and emerging platforms and services for online communication and collaboration are used to take part in global conversations.

In online social networks, the lines between public and private, personal and professional can be perceived to be blurred. It is expected that all who participate in social media on behalf of the EMSB, understand and adhere to the following guidelines, they should:

- Post meaningful, respectful comments – in other words, no SPAM and no offensive remarks. Always pause and think before posting. What a person publishes is widely accessible and will be available to others. Therefore, the posting or electronic publication of the content should be carefully considered for its short and long term implications and impacts.
- Respect proprietary information, context, and confidentiality;
- When disagreeing with others' opinions, keep it appropriate and polite;
- Use your real names, identify their role at the EMSB;
- Clearly identify if they have a vested interest in the topic being discussed.

ANNUAL REPORTING

The Council of Commissioners shall receive on an annual basis a report from T.A.S.C. on the application of this policy.

APPENDIX I – GLOSSARY

ICT Stakeholder: denotes any individual or organisation that makes use of EMSB-managed technology resources, either directly or indirectly.

ICT Equipment or Devices: denotes any physical piece of technology provided or managed by the EMSB. These include but are not limited to, computers, desktop telephones, cellular telephones, interactive white boards and digital projectors.

Infrastructure: denotes the foundation of a computing environment that controls access to and flow of information within the organisation such as servers and network switches.

ICT Systems: Refers to all EMSB Equipment and Infrastructure.

User: denotes any individual or organisation that makes direct use of EMSB-ICT Systems.

Software: denotes the collection of programs and related data that provide the instructions telling a computer what to do.

Peer-2-Peer: computing or networking: denotes a distributed application architecture that partitions tasks or workloads between peers. As with most network systems, unsecure and unsigned codes may allow remote access to files on a victim's computer or even compromise the entire network.

Anonymous Internet Services: denotes an Internet service that hides the site to which they are connecting. These services are used to bypass any access restriction/filtering that are in place.