| Commission scolaire English-Montréal<br>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.

# APPENDIX II – AGREEMENT FORM – ELEMENTARY STUDENTS

- When using school computers, I will use good manners, use appropriate language and not look at or use anyone else's work without permission;
- I shall not give out personal information such as my address, telephone number, parents' work addresses or telephone numbers, credit card;
- I shall not give out the name and address of my school without permission;
- I shall tell my teacher right away if I come across any information that is inappropriate or makes me feel uncomfortable;
- I shall never send my picture or anything else without first checking with my parents and /or teacher;
- I shall not respond to any messages that are mean or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do, I will tell my teacher right away;
- I shall not give out my password to anyone (even my best friends) other than my teacher;
- I shall never agree to get together with someone I "meet" on-line;
- I shall talk with my parents about the rules for going on-line;
- I understand that anyone can read messages I send and that my work on the computer is not private.

I have read and I understood the rules and promise to follow them. If I do not follow these rules I know that I may have my computer privileges restricted or taken away.

Student's School: _____

Grade: _____

Student Name (please print): _____

Student Signature: _____

Date: _____

Date of Birth: _____

A complete version of the Policy is available on the school board Web site at www.emsb.qc.ca

**Parent or Guardian Consent**

I have read and understood the Policy on the Access & Appropriate Use of Information and Communication Technology. I grant permission for my child or charge to access networked services such as email and the Internet. I will do my best to ensure that my child adheres to this policy to the best of my abilities.

Name of Parent or Guardian (please print): _____

Signature of Parent or Guardian: _____

Date: _____

# APPENDIX III – AGREEMENT FORM – STUDENTS UNDER 18 (HIGH SCHOOL OR AEVS CENTRE)

## Student Agreement

I have read and I understood the Policy on the Appropriate Use of Information and Communication Technology. I agree to abide by it and understand that any violation of any provision may result in the loss of access privilege and school or centre sanctions.

Student's School or Centre: _____

Level or Program: _____

Student's Name (please print): _____

Student's Signature: _____

Date: _____

Date of Birth: _____

A complete version of the Policy is available on the school board Web site at www.emsb.qc.ca

## Parent or Guardian Consent

I have read and understood the Policy on the Appropriate Use of Information and Communication Technology. I grant permission for my child or charge to access networked services such as email and the Internet. I will try to ensure that my child adheres to this policy to the best of my abilities.

Name of Parent or Guardian (please print): _____

Signature of Parent or Guardian: _____

Date: _____

# APPENDIX IV – AGREEMENT FORM – STUDENTS 18 YEARS & OVER

## User Agreement

I have read and I understood the Policy on the Appropriate Use of Information and Communication Technology. I agree to abide by it and understand that any violation of any provision may result in the loss of access privilege and school or centre sanctions.

Student's School or Centre: _____

Level or Program: _____

Student's Name (please print): _____

Student's Signature: _____

Date: _____

Date of Birth: _____

A complete version of the policy is available on the school board Web site at www.emsb.qc.ca

# APPENDIX V – AGREEMENT FORM – EMPLOYEE

## Employee Agreement

I have read and I understood the Policy on the Access and Appropriate use of Information and Communication Technology. I agree to abide by it and understand that any violation of any provision may result in the loss of access privilege and disciplinary measures.

Employee's School, Centre, Department: _____

Employee's Name (please print): _____

Employee's Signature: _____

Date: _____

A complete version of the policy is available on the school board Web site at www.emsb.qc.ca

# APPENDIX VI – INTERNET FILTERING

Following is a list of Internet elements and how the EMSB will filter each.

## Deny Access

Botnets
Keyloggers
Phishing & Frauds
Spyware
Proxy Avoidance
URL Translation sites
Web & Email SPAM
Remote Access
Peer-to-Peer File Sharing
Unwanted Software
Advertisements
Malicious Web sites
Online Brokerage
Pay-to-Surf
Adult Material
Illegal or Questionable
Hacking
Web Hosting
Personal Network Storage and Backup
Internet Auctions
Personals and Dating
Sport Hunting and Gun Clubs
Tasteless
Weapons
Freeware and Software Download

## Allow Access

These are allowed ONLY for purposes directly related to an individual's work or education based activity -

Business & Economy
Education
Government
Organisational Email
News & Media
Special Events
YouTube
Message Boards and Forums
Information Technology
Search Engines and Portals
General Email
Text and Media Messaging
Professional and Worker Organisations
Service and Philanthropic Organisations
Social and Affiliation Organisations
Society and Lifestyles
Mail and Collaborative Tool
Advocacy Groups
Health
Web Chat
Prescribed Medications
Restaurants and Dining
Social Networking and Personal Sites
Sports
Travel
Vehicles
Internet Telephony – Skype
Internet Radio and TV
Streaming Media
Instant Messaging
Message Boards and Forums
Prescribed Medications
Entertainment
Job Search
Hobbies
Shopping
Real Estate

# APPENDIX VII – EMPLOYEE ACCOUNT CHANGE REQUEST

## User Accounts

User account changes include requests to; setup a new user, changes to existing accounts (i.e. add or remove accesses to systems such as GPI, DOFIN, etc.), deactivating accounts temporarily, requesting a new phone number and removing accounts. Requests of this type are to be made by the person's direct supervisor or director of service using the "**Employee Account Change Form - ePaper.pdf**".

The completed form it is to be sent via email to ITSupport@emsb.qc.ca for processing providing a minimum of five (5) business days notice. The form is found on the forms section of the EMSB Intranet.

## Service Requests

These represent requests for services outside of the daily support elements, i.e. setting up equipment for a workshop, moving equipment connections from one location to another, etc. Requests of this nature are to be submitted via email to ITSupport@emsb.qc.ca providing a minimum of ten (10) business days for processing.

## Sample form

This form is to be completed by the employee's immediate supervisor or the related director of service whenever a computer access is to be created, removed or modified. Forward this completed form via email to **ITsupport@emsb.qc.ca** allowing five (5) business days for processing.

**Request Type:** ◯ New ◯ Departure ◯ Temporary Leave ◯ Change

**Date Required:** (yyyy-mm-dd)

**First Name:**

**Last Name:**

**Email Address:** (existing users only)

**Department Name:**

**Disable Account:** ◉ No ◯ Yes From: (yyyy-mm-dd) To: (yyyy-mm-dd)

**Delete Account:** ◉ No ◯ Yes Date: (yyyy-mm-dd)

**Special Software Needs:** ◯ GPI ◯ GPI-Internet ☐ SPI ☐ DOFIN ☐ PAIE ☐ REGARD ☐ AVANT GARDE ☐ JADE ☐ Portal

Other:

**Computer:** ◯ New ◯ Transfer from:

**Office Phone:** ◯ New ◯ Transfer from:

**Comments:**

**Submitted by:** (supervisor's name) **Date:** (yyyy-mm-dd)

# APPENDIX VIII – EMAIL USER GUIDE

## Introduction

Electronic mail (email) has become an important means of communicating quickly and easily with a large number of people. However email can be misused and abused. Here are a few do's and don'ts to make using emails safer and more effective.

## Email Security

- Emails are not necessarily private. Do not include anything in an email that you would not want other people to see – in particular, be aware that the laws on defamation apply to emails.
- Before sending messages that contain sensitive or personal information you might consider whether emailing them is appropriate.
- Before you forward an email, make sure that all recipients need to receive the message. In addition, be careful when forwarding sensitive or confidential information. Never forward proprietary information to external audiences or to unauthorised recipients. Before clicking the Send button, review whether a message's contents are appropriate for each listed recipient.
- **Viruses**: are often spread through email. You can reduce the spread of email viruses by opening email only from trusted sources and opening only attachments you're expecting. If you receive a message of which you are suspicious DO NOT OPEN IT – it might be a Virus. In particular only open attachments you are sure are from a reliable source.
- **Phishing**: Never respond to emails that request personal security information. A type of spam which has been nicknamed 'Phishing' is becoming increasingly common, where you receive a 'spoofed' email that appears to come from a legitimate website that you have dealings with, such as a financial institution. It may ask you to verify your account details by going to a link in the email, but a legitimate organisation, including the EMSB ITS group, will never ask you for this type of information.

  Online banking and e-commerce are generally safe, but you should always be careful about divulging personal and corporate information over the Internet. Phishing messages often boast real logos and appear to have come from the actual organisation, but those messages are frequently nothing more than copyright infringements and faked addresses. If you suspect a message possesses any credibility, you are much safer calling the individual to confirm the authenticity.

  Although the EMSB has implemented a filtering system, the attacks are becoming very sophisticated, and it is hard to differentiate a phishing email from a legitimate one, so our systems may not identify them as

SPAM. They often contain a link to a fake website that looks just the same as the real site, but has been set up to steal personal information. For more information and advice, visit:

http://www.antiphishing.org/resources.html#advice.

- **SPAM**: Reduce the amount of spam you receive by being cautious where you post your email address. Never forward chain messages, which often reveal coworkers' and colleagues' email addresses to other parties. Use caution when accepting email offers or agreeing to accept mailings from vendors; subscribe only to Web sites and newsletters you really need.

  Do not divulge coworkers' email addresses to vendors, friends, or others outside the organisation. Verify that recipients listed in the To and CC fields should be receiving messages and that you will not be revealing others' email addresses in the process. Do not post your or coworkers' email addresses on Internet forums, social networking services or sites, chat rooms, or other public areas.

## Sending Email

- Keep messages short and simple – the usual rules of good writing apply; be clear and concise, express one idea per paragraph or section, check your spelling and use of proper grammar
- Only use special formatting in emails; i.e.: colours, bold, italic, etc., if you know the recipient's system can read these details, such as people using Outlook, Lotus Notes, Hotmail, etc. Some older email systems cannot read these messages at all, and some may display them as plain text, so any formatting you have applied will be lost. In this case, use the plain text format instead. This is especially true if you are using the formatting to convey a special message or emphasis.
- Be careful when using humour, sarcasm and irony, particularly if the message is to someone who does not know you. "Emoticons" (smileys) are often used to convey humour, etc.
- Long messages (over 250 lines) might not be easy to read – an attachment might be better. (See below guide on sending attachments)
- Covering multiple topics in one note involves less sending and hence less e-mail traffic and volume. However, your recipient might overlook one or more of those topics. It's better to keep to one topic per message. If you do need to cover more than one topic within the email ensure this is indicated in the subject line.
- A forwarded or redirected message will generally have sections by different authors. Each section should clearly identify who wrote it and this information should be maintained as the message is passed on

- Forwarded messages can grow in size, particularly if several different people have forwarded it and added comments – be careful if you edit the message
- Before forwarding messages you might consider notifying the sender of the message. This becomes more important as the sensitivity or the message contents increases.

## Email Attachments

Attaching files to an email message is a very convenient way to distribute documents. But it may be difficult or awkward for the recipient, keep the following points in mind to make life easier for them. They are particularly important if you are sending to many people as when using distribution lists.

- Do not use attachments when a plain text will do; a simple memo may be better sent as text within the email message. It is both quicker and easier for recipients to read the text in the email message than to open an attachment.
- Make sure that recipients can read your attached files; make sure all recipients have the same version of the application in which you created the document. If this cannot be determined accurately use a universal format such as Adobe's PDF.
- Keep the size of attachments to a minimum. The EMSB has implemented a high speed network throughout our facilities, but this is not the case for everyone. A recipient may not be able to read a large attached file. The total maximum message size allowed for all incoming or outgoing messages is 20MB.
- When forwarding or replying to messages with attachments, unless absolutely necessary, avoid leaving the attachment in the email. This increases the size of the email, uses limited organisational resources unnecessarily, and makes the message difficult to follow.

## Professional Messages

Always include a descriptive subject line, summarise the message without being wordy or vague. Long subjects tend to be skimmed or ignored, and are not always properly displayed in email viewers.

It's easy to convey the impression that you're unprofessional or careless if you don't follow some basic principles of good business writing. Make sure you follow proper grammar and sentence structure when composing and responding to messages and use a spell checker. Do not type in all CAPITAL letters; it creates the effect of shouting. Break your message into paragraphs for logic and readability.

Before clicking the Send button, give it a final once-over. Reread the entire email, checking it for grammatical errors, punctuation mistakes, and typos. Make sure your tone is appropriate for the message. Email messages have a tendency to sound cold;

emotions are difficult to convey in the written word. For this reason avoid elements that are vague or may be interpreted differently by different readers. Providing basic facts, actions, or directions is best; call the individual should a more detailed explanation/clarification be required.

When using the **Reply** function to simplify addressing of a new email to someone make sure to adjust the Subject line accordingly. Leaving the subject line unchanged may cause confusion for the reader as well as a misinterpretation of the information contained within the message.

Most email windows don't have the same size and range of a printed page. Use shorter paragraphs to better get your point across. It will be easier for readers to scroll through your message, making it easier for them to absorb what you are saying.

Proper Message Addressing (To, CC, and BCC)

The primary person to which the message is being addressed, as well as the one from whom you are expecting a response, should be the first listed on the **To** line, the others are there as backup. The carbon copy (CC) and blind carbon copy (BCC) features found in most email clients allow you to send copies of an email to others that need to keep informed but who are not the primary recipients and not directly affected by the information in the message.

When copying others, be certain the email message pertains to them. If you use email distribution lists, verify that all of the members of the list should receive the email; remove those who don't need to be included. Use the BCC feature sparingly. If sensitive topics require BCCing others, it may be best to discuss the matter in person.

### Do not be a Party to a Flame War

Flame wars are heated email exchanges that are more emotional than reasoned, and they have no place in professional communications. If you receive a flame or suddenly find yourself in a flame war, take a little time before responding, if you respond at all. Think about the situation and reply rationally not emotionally. This is usually done best in person.

### Know when to use Email (and when not to)

Email should not be used to replace a conversation. When used in this way the activity is unnecessarily complicated, lengthy, in most case resolves nothing, and is an inappropriate use of scarce organisational resources. Nor should complicated subjects be “discussed” in this manner. Instead set up a short meeting to address the issue in person.

Email is also a poor stand-in for conversation when conducting critical, difficult, and/or unpleasant discussions, such as issues related to human resources matters. Touchy communications are best handled in person.

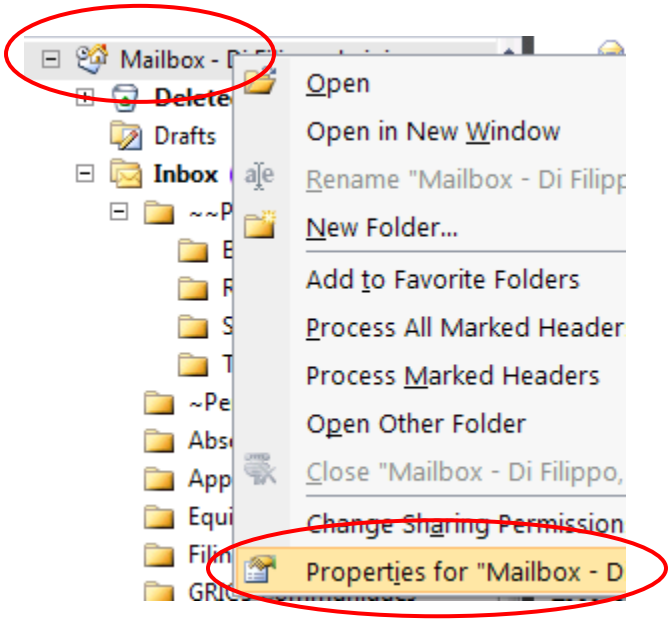
## Managing Your Mailbox

EMSB email users have been allocated 500MB of storage for email messages. This includes all of the space occupied by not only incoming messages but also, calendar entries, sent messages, filed messages in user created folders, and deleted messages.

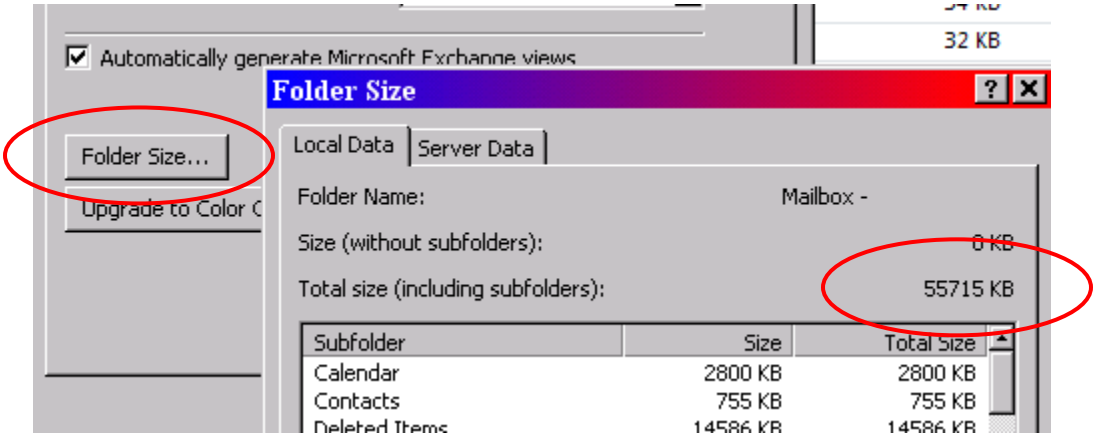
Sort the messages by priority, subject, date, sender, and other options to help find important email that requires your attention. Proper email etiquette dictates that you respond to all email in a timely fashion. Generally speaking, you should respond to all professional email within a business day, even if it is just to say you've received the message and will look into the matter. Occasionally, you may receive an email thread that contains responses from several people; always read the entire thread before responding.

## Check the Size of Your Mailbox

- Open Outlook
- Right click on Mailbox then select Properties from the drop down list:

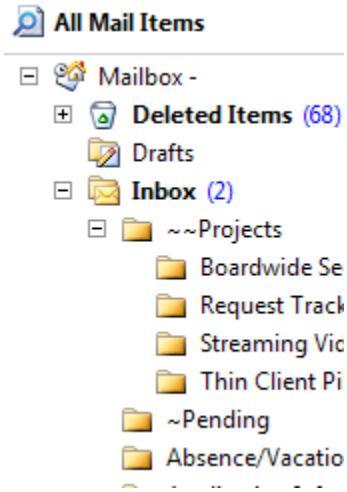


- In the window that opens Click on the Folder Size button at the bottom of the screen. This will show you the total size of your mailbox.

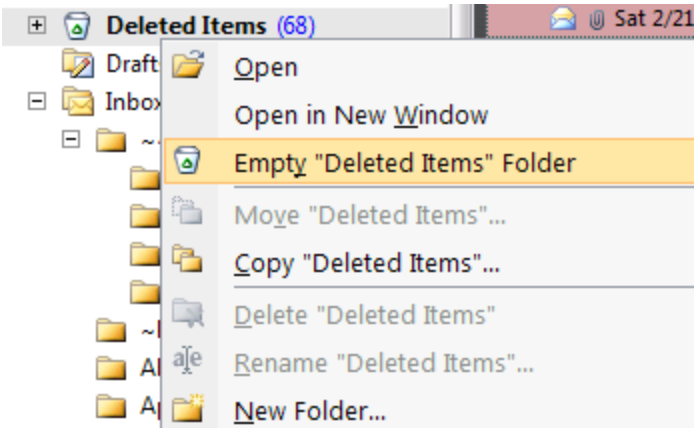



## Mailbox is Full

- Delete unimportant emails or messages you no longer need
- Reduce the size of your mailbox: Your mailbox is not only your Inbox, but includes all the folders listed; folders you created, Deleted Items, Sent Items, Outbox, etc.




- Check the following folders and delete whatever is not necessary. Highlight the items to be deleted, then press SHIFT and Delete together to permanently delete the items.
    - **Sent Items** folder (these items can be filed in other folders should they need to be retained) otherwise delete the message
    - **Outbox folder**
    - **Deleted Items;** usually you can remove all the contents of this folder. To do this, right click on the Deleted Items folder and select Empty from the pop down list




- Check your Inbox and any other folders in your Mailbox, (those listed directly under your name); Delete old messages and anything else you don't need to keep.

## Requesting Additional Space

Mail messages for EMSB staff are held on the central Exchange servers managed by ITS. Storage space is not infinite so in order to keep costs down and to simplify administration, a quota of 500MB has been applied to all staff. This should be sufficient for the majority of people, provided they manage their mailbox as outlined above.

In exceptional circumstances, if the quota is not sufficient for an individual to carry out their job effectively, an increase may be requested together with a clear justification of the need. ITS may have to pass on the costs of increased quotas in the future, but at present there is no additional cost.

Any request for an increased quota must come from the individual's immediate supervisor. This must confirm that, as part of their job, the person in question has to be able to access large volumes of emails. The request must be made in writing to the Director of ITS. Any increase in limit, as well as the duration of the arrangement will be at the discretion of ITS.