COMMISSION SCOLAIRE
Eastern Shores
SCHOOL BOARD

POLICY ES-250

ACCESS AND APPROPRIATE USE OF TECHNOLOGY AND COMMUNICATION TECHNOLOGY

Adopted on : 22-06-2022

Resolution: C22-06-872

Contents

1. POLICY STATEMENT 3
2. RESEARCH-BASED RATIONALE 3
3. FIELD OF APPLICATION 3
4. PURPOSE 4
5. PRIVACY AND PROPRIETARY RIGHT 4
6 EQUIPMENT, SOFTWARE, AND SERVICE REQUESTS 4
6.1 Equipment 4
6.2 Software 5
7 ROLES AND RESPONSIBILITIES All ICT STAKEHOLDERS 5
7.1 Schools and Centers 6
7.2 Students 6
8 PROTECTION OF CONFIDENTIAL, PROPRIETARY AND PERSONAL INFORMATION 7
9. LIABILITY 7
10. ENFORCEMENT 7
11. SYSTEM ACCESS MANAGEMENT 8
12. PASSWORDS FOR ALL USERS 8
13. INTERNET USAGE 8
13.1 Authorized Personal Use of ESSB Internet Access – Employees 8
13.2 Authorized Personal Use of ESSB Internet Access – Students 8
13.3 Internet Privacy 8
14. EMAIL USAGE 9
15. EMAIL PRIVACY 9
16. INAPPROPRIATE USE OF EMAIL 9
17. SOCIAL MEDIA USAGE 9
APPENDICES 10
APPENDIX I – GLOSSARY 10
APPENDIX II - Agreement Form - Elementary Students 11
APPENDIX III – Agreement Form – Students Under 18 12
APPENDIX IV – Agreement Form – Students 18 Years & Over 13
APPENDIX V – Agreement Form – Employee Agreement 14
APPENDIX VI – EMAIL USER GUIDE 15
REFERENCES 19

1. 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 Eastern Shores School Board (ESSB) 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 ESSB ICT Systems;
- Continuously sensitize all stakeholders to the appropriate and secure use of ICT;
- Restrict access to internet sites with inappropriate content.

2. RESEARCH-BASED RATIONALE

Michael Fullan (2013) refers to the integration of pedagogy, technology and change knowledge as a triad known as 'stratosphere'. Although each of these factors is individually important at ESSB, the potential synergy of the three, in combination in a contemporary coastal classroom, is even more so.

Technology can help us by "opening up the world to deeply engaged learning and worldwide collaborative problem solving" (p. 14). We need to "capitalize on [students'] digital prowess to inspire confidence, curiosity, persistence, and desire for knowledge" (p. 43). "Changes in technology and pedagogy are becoming dramatically compelling." (p.5). This Access and Appropriate Use policy document helps align the two and provides a framework to make them synergistic.

Fullan's solution to implementing stratosphere is threefold:

1. Focus on learning;
2. Let technology permeate;
3. Engage the whole system (p. 74).

Encouraging more use of technology by students and teachers requires a policy framework to guide these changes. This Access and Appropriate Use of Information and Communication Technology policy provides the framework to synthesize pedagogy, technology, and change knowledge to provide opportunities for ESSB students to use technology (devices and networks) efficiently, safely and appropriately.

3. FIELD OF APPLICATION

This ESSB ICT Access and Appropriate Use of Information and Communication Technology policy, hereafter known as the "Policy", applies to the telecommunication and computing infrastructure, equipment and services provided or managed by the ESSB, or any external systems accessed while using these services, including any software installed or running within ESSB-managed systems. Additionally, this applies to any ICT, which may presently, or in the future, be provided through other sources for use at the ESSB either directly or remotely. The Policy also applies to all ICT stakeholders (employees, students, Commissioners, parents, general public, etc.) that access or use ESSB ICT.

4. PURPOSE

The ESSB recognizes 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 ESSB administrative and educational activities;
- Define the respective responsibilities of all ESSB ICT stakeholders with respect to the effective, appropriate, legal, ethical, educational, and employment related use of ICT;
- Respect the privacy of personal and organizational information.

5. PRIVACY AND PROPRIETARY RIGHT

1. The ESSB extends the privilege of reasonable personal use of the ESSB's ICT Systems to all employees;
2. The ESSB 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 ESSB's ICT Systems is extended to its employees, the ESSB 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 ESSB's ICT Systems;
4. Employees should be aware that any work created or stored on ESSB ICT Systems, whether or not related to their job function, remains the property of the ESSB, 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 ESSB ICT Systems remains the property of the student unless there is a prior agreement to the contrary with the ESSB.

6 EQUIPMENT, SOFTWARE, AND SERVICE REQUESTS

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

6.1 Equipment

- Purchases of ICT Equipment must be processed through ITS via an email request to tech.support@essb.qc.ca, with a minimum of ten (10) business days' notice;
- Purchases of ICT Equipment will be determined by the classification of employment as outlined in the Board owned computer devices document – "Organizational Guide – 02.doc".
- Installation or configuration of new or existing ICT Equipment must be processed through ITS via an email request to tech.support@essb.qc.ca with a minimum of ten (10) business days' notice;
- Cabling additions or modifications for ICT Equipment must be processed through ITS via an email request to tech.support@essb.qc.ca with a minimum of ten (10) business days' notice.

6.2 Software

- Purchases of software, either administrative or educational in nature, must be processed through ITS via an email request to tech.support@essb.qc.ca with a minimum of ten (10) business days' notice;
- New software must be approved by the director of the department prior to being purchased. The request may be sent via email to ITS for processing at tech.support@essb.qc.ca. Timelines will vary depending on the complexity of the software being evaluated;
- Installation or configuration of software must be processed through ITS via an email request submitted to tech.support@essb.qc.ca with a minimum of ten (10) business days' notice.

7 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 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;
3. Take reasonable precautions to prevent unauthorized access to ESSB ICT Systems. Such precautions include keeping login identifiers and passwords confidential, and locking or preventing unauthorized access to your computer when left unattended for extended periods of time;
4. Refrain from storing personal files on ESSB equipment;
5. Ensure one drive is connected to office 365 for file backups;
6. Report to tech.support@essb.qc.ca any material received or stored in any manner (text, images, sound, etc.) which appears to be in violation of the Policy;
7. Respect and protect personal and confidential information regarding themselves and others;
8. Refrain from harming, attempting to harm, or destroying ESSB data;
9. Refrain from obtaining, by any means, access to any system, service, privilege or electronic material to which they are not authorized;
10. Refrain from violating Canadian copyright laws;
11. Refrain from installing unauthorized software on ESSB-managed computers;
12. Refrain from using Peer-to-Peer Services (P2P) or any evolution thereof;
13. Respect all laws and policies which specify appropriate use of computers and other telecommunications equipment;

14. Refrain from using ESSB 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;
15. Request permission from School or Centre Administrators, as applicable, before releasing information that may appear to be sanctioned by the ESSB or is linked to official ESSB web sites;
16. Refrain from transmitting unsolicited bulk information (SPAM), including junk mail, advertising, jokes, solicitation, chain letters, virus alerts, etc.;
17. Be aware that we share a fixed amount of bandwidth. Users need to be respectful of the amount of bandwidth used in schools and centers. Specific examples include: Avoid downloading large amounts of video content. Avoid connecting every device in a school or center simultaneously.

7.1 Schools and Centers

It is the responsibility of the School or Adult Education 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 one of the applicable Annexes II, III or IV in 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 center guidelines;
6. Use of ESSB ICT Systems is supervised by ESSB employees or those authorized by the school to supervise the users;
7. Monitor and enforce the respectful use and care of ESSB devices (Chromebook, laptop, Tablet, etc.) that are assigned to students.

7.2 Students

It is the responsibility of the student to:

1. Submit a signed Consent or Agreement Form (Appendix II, III or IV) 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 authorized ESSB personnel;
3. Only access appropriate content relevant to education and in line with the objectives of class assignments and related to courses of study set out by their teachers;
4. Immediately report to the teacher, supervisors, or administrator, any information, message or web site that is inappropriate or makes them feel uncomfortable;
5. Obtain permission from the supervising teacher or educator before printing;

6. Respect careful and appropriate handling of devices provided to them by ESSB. Respect their own device(s) and those of others (examples: Chromebook, laptop, tablet, desktop computer, and any device in their possession);
7. Typical manufacturer warranties apply to faulty devices, not damage caused by user neglect or abuse (example: If the device just stops working or cannot be recharged). Students must notify their teacher who in turn should notify Tech Services at tech.support@essb.qc.ca of any such problems with the device;
8. Please note that devices damaged or broken due to inappropriate handling or abuse by students will be replaced at the expense of the student.

8 PROTECTION OF CONFIDENTIAL, PROPRIETARY AND PERSONAL INFORMATION

Unless authorized to do so, employees or third parties working on behalf of the ESSB are prohibited from transmitting confidential or nominative information through any electronic medium to any party. Employees or third parties working on behalf of the ESSB may not access, send, receive, solicit, print or copy confidential or proprietary information regarding the organization, employees, suppliers, students, or other associates unless so designated by virtue of their job description or authorized 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 ESSB, 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 that the originator would reasonably expect to be kept private.

9. LIABILITY

The ESSB is not responsible for any loss or damage to users' data or storage devices, or for any other problems incurred as a result of using its ICT Systems.

10. ENFORCEMENT

Instances of probable inappropriate use may be investigated. The ESSB shall act discreetly and in a confidential manner in conducting such investigations. Investigations that uncover inappropriate use may result in the ESSB:

1. Cancelling or limiting access to facilities or ICT Systems;
2. Disclosing information found during the investigation to ESSB authorities, or law enforcement agencies;
3. Disciplinary measures involving employees could include possible dismissal, according to collective agreement procedures, applicable laws and/or Schools' or Centers' behavior codes.

4. Disciplinary measures involving students could include revoking ESSB email and access to ESSB devices and school internet;
5. A user will be responsible for damages to ESSB software and/or equipment resulting from gross negligence or intentional actions;
6. In those instances of probable inappropriate use by a Commissioner, the Director General shall refer the matter to the Ethics Commissioner.

11. SYSTEM ACCESS MANAGEMENT

All ESSB internet access networks must have appropriate user IDs and passwords to ensure access is restricted only to authorized individuals. Access authorization is to follow the process identified in related Procedure Statements.

12. PASSWORDS FOR ALL USERS

All users should regularly change passwords and practice best Digital Citizenship regarding safety and sharing of information. Each student's password can be reset by ITS.

13. INTERNET USAGE

The ESSB 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 ESSB. Any user who violates these rules and policies is subject to disciplinary action.

13.1 Authorized Personal Use of ESSB Internet Access – Employees

Employees may access Internet resources for specified personal use during non-work hours. Employees are prohibited from using ESSB 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.

13.2 Authorized Personal Use of ESSB 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 ESSB internet access to operate a business, solicit money for personal gain, campaign for political causes or candidates, or promote or solicit funds for religious or other personal causes.

13.3 Internet Privacy

Access to the internet is provided by the ESSB and, as such, the ESSB 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 ESSB.

14. EMAIL USAGE

The ESSB provides employees and students with electronic communications tools, including an ESSB email system. This policy applies to the on-site or remote access and use of the ESSB email system. The ESSB email rules and policies apply to all users who have an ESSB email address. Any user who violates these rules and policies is subject to disciplinary action. The ESSB allows email access for activities and communications that support and relate to the mission, vision and strategic plan of the ESSB. Employees may use the organization's email system for personal use only in accordance with this policy. For email best practices guidelines see the Email User Guide (Appendix VI).

15. EMAIL PRIVACY

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

16. INAPPROPRIATE USE OF EMAIL

Employees and Students are prohibited from using ESSB 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.

17. 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 blurred. To the extent that speech on social media is part of the public domain, there is nothing to prevent an employer from monitoring employees' activities on Facebook, Twitter and other social media. An employee's duty of loyalty extends beyond working hours and survives even after the employment relationship is severed. Accordingly, an employee may not, even outside of work hours and using his or her own computer equipment, disseminate confidential information about his or her employer or its stakeholders, take positions or make public statements that may affect the employer's reputation or business, or harass, intimidate or threaten an officer or co-worker. It is expected that all who participate in social media, understand and adhere to the following guidelines, they should:

- **Post meaningful, respectful comments** (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 their real names and identify their role at the ESSB;
- Clearly identify if they have a vested interest in the topic being discussed.

APPENDICES

APPENDIX I – GLOSSARY

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.

AEVS: Adult Education and Vocational Services

ESD: Educational Services Department

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

ICT Systems: Refers to all ESSB Equipment and Infrastructure.

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

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.

Social Media: is the social interaction among people in which they create, share or exchange information, ideas, and pictures/videos in virtual communities and networks.

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

Stakeholder: denotes any individual or organization that makes use of ESSB-managed technology resources, either directly or indirectly.

User: denotes any individual or organization that makes direct use of ESSB-ICT Systems.

Videoconferencing: telecommunication technology which allow two or more locations to communicate by simultaneous two-way video and audio transmissions. (Examples include SKYPE, Google Hangouts, etc.).

APPENDIX II - Agreement Form - Elementary Students

COMMISSION SCOLAIRE EASTERN SHORES
EASTERN SHORES SCHOOL BOARD

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 above 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.essb.qc.ca

Parent or Guardian Consent

I have read and understood the Policy on the Access and 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

COMMISSION SCOLAIRE EASTERN SHORES
EASTERN SHORES SCHOOL BOARD

AGREEMENT FORM – STUDENTS UNDER 18
(HIGH SCHOOL OR Adult Education CENTRE)

Student Agreement

I have read and I understood the Student portions of 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 school or center 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.essb.qc.ca

Parent or Guardian Consent

I have read and understood the Policy on the Access and Access and 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

COMMISSION SCOLAIRE EASTERN SHORES
EASTERN SHORES SCHOOL BOARD

AGREEMENT FORM – STUDENTS 18 YEARS & OVER

Student Agreement

I have read and I understood the Student portions of 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 school or center sanctions.

Student's School or Centre: _____

Level or Program: _____

Student's Name (please print): _____

Signature: _____

Date: _____

Date of Birth: _____

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

APPENDIX V – Agreement Form – Employee Agreement

COMMISSION SCOLAIRE EASTERN SHORES
EASTERN SHORES SCHOOL BOARD

AGREEMENT FORM – EMPLOYEE Agreement

I have read and 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, and 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.essb.qc.ca

APPENDIX VI – 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 unauthorized 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 organization, including the ESSB 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 organization, 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;

SPAM: Reduce the amount of spam you receive by being cautious where you post your email address. Never forward chain messages, which often reveal co-workers' 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 organization. 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.

Although the ESSB 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/overview/.

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, and check your spelling and use of proper grammar;

Only use special formatting in emails; i.e.: colors, 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 humor, sarcasm and irony, particularly if the message is to someone who does not know you. "Emoticons" (smileys) are often used to convey humor, 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. ESSB 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;

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 organizational resources unnecessarily, and makes the message difficult to follow.

PROFESSIONAL MESSAGES

Always include a descriptive subject line, summarize 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 is 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 "BCC" to others, it may be best to discuss the matter in person.

Do not be involved in an exchange of angry or abusive messages between users (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 organizational 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 resource matters. Touchy communications are best handled in person.

MANAGING YOUR MAILBOX

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 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.

REFERENCES

Fullan, Michael. *Stratosphere: Integrating Technology, Pedagogy, and Change Knowledge.* Don Mills, Ont.: Pearson, 2013. Print

APWG: Worldwide coalition unifying the global response to cybercrime: http://www.antiphishing.org/resources/overview/

http://www.oxforddictionaries.com/definition/english/flame-war

This document was created based on the English Montreal School Board Acceptable Usage Policy. http://www.emsb.qc.ca/en/governance_en/pdf/BoardPolicies/DirectorGeneral/DG-25%20ICT%20Access%20and%20Appropriate%20Use%20Feb%2027%202012.pdf