ACCEPTABLE USE OF THE WIDE-AREA NETWORK AND THE INTERNET

Background

Mother Earth's Children's Charter School (MECCS) relies on its computer network to conduct, in part, its business. To ensure that its computer resources are used properly by its staff, independent contractors, agents, students, volunteers and any other computer users, the Superintendent has created this Acceptable Use of the Wide Area Network and the Internet procedure.

More specifically, the school has implemented an electronic communications system (wide-area network or the "WAN") that provides access to the Internet and allows unprecedented opportunities for students, staff, independent contractors, agents, volunteers, and any other school computer users to communicate, learn, access, and publish information.

The school believes that the resources available through this network, and the skills that students will learn in using it, are of significant value in the learning process and their success in the future. As a result, the school supports the use of the WAN and the Internet to facilitate the smooth operation of the school and to facilitate learning and teaching through interpersonal communications, access to information, research, and collaboration.

The rules and obligations described in this procedure apply to all users (the "Users") unless exceptions are specifically set out in this procedure, of the school's computer network, wherever they may be located, either upon or outside school property. Violations will be taken very seriously and may result in disciplinary action, including possible termination, and civil and criminal liability.

Definitions

Computer Resources: refers to the entire MECCS computer network. The term specifically, includes, but is not limited to: host computers, file servers, application servers, communication servers, mail servers, fax servers, Web servers, workstations, stand-alone computers, laptops, software, data files and all internal and external computer and communications networks (for example Internet, online services, value-added networks, e-mail systems) that may be accessed directly or indirectly from our computer network.

Users**:** refers to all staff members, independent contractors, consultants, temporary workers, students, volunteers and other persons or entities who use MECCS computer resources.

Procedures

1. The Computer Resources are the property of MECCS and may be used only for legitimate business purposes or for purposes referred to in this procedure. As a general rule, Users are permitted access to the Computer Resources to assist them in performance of their jobs or in fulfillment of their duties or tasks.

2. Use of the computer system or Computer Resources is a privilege that may be revoked at any time. The use of the Computer Resources is not a right. Inappropriate, unauthorized and illegal use will result in the automatic cancellation of that privilege and the Superintendent or designate will take appropriate disciplinary action.

3. The use of the Computer Resources shall be consistent with the mission of MECCS and provincial curriculum requirements, taking into account the varied instructional needs, learning styles, abilities, and developmental levels of students.

4. Use of the Computer Resources and the network by students, staff, independent contractors, consultants, temporary workers, volunteers and other persons or entities who use the Computer Resources must be in support of educational objectives, or of the effective operation of MECCS. (The Superintendent or designate maintains the sole discretion to decide what constitutes "effective operation of MECCS) The Superintendent or designate reserves the right to prioritize use and access to the Computer Resources.

5. **All** use of the Computer Resources by any person must be in conformity with federal, provincial, and municipal laws, and in accordance with MECCS policies and procedures.

6. The availability of electronic information to students, staff, independent contractors, consultants, temporary workers, volunteers and other persons or entities who use MECCS computers does not imply endorsement of the content by the school, nor does the school guarantee the accuracy of information, through the Computer Resources, on the Internet.

7. All students, staff, independent contractors, consultants, temporary workers, volunteers and other persons or entities who use MECCS computers shall be responsible for any unauthorized charges, fees, costs, damages, or injuries resulting from their use of the Computer Resources, or in accessing the Internet.

8. In using or accessing the Computer Resources, Users must comply with the following provisions:

    8.1 NO EXPECTATION OF PRIVACY

    No expectation of privacy. The computers and computer accounts given to Users by the school are to assist them in performance of their jobs. Users should not have an expectation of privacy in anything they create, store, send, or receive on the computer system. The computer system belongs to the school and may be used only for business purposes, subject to any exceptions in this procedure.

Waiver of privacy rights. Users expressly waive any right of privacy in anything they create, store, send, or receive on the school computers and Computer Resources or through the Internet or any other computer network. Users consent to allowing school personnel to access and review all materials Users create, store, send, or receive on the computer, the Computer Resources, or through the Internet or any other computer network. Users understand that the school may use human or automated means to monitor use of its Computer Resources.

As there is no reasonable expectation of privacy in the User's use of MECCS computers, Internet, e-mail, or Computer Resources, the school may monitor any and all aspects of its computer system, including, but not limited to, monitoring sites visited by Users on the Internet, monitoring chat groups and newsgroups, reviewing material downloaded or uploaded by Users to the Internet, and reviewing e-mail sent and received by Users.

No privacy in e-mail. All Users are never to consider electronic communications to be either private or secure. E-mail sent to non-existent or incorrect usernames may be delivered to persons that the User never intended. E-mail is a record under the *Freedom of Information and Protection of Privacy Act*.

8.2 STAFF MEMBER'S DUTY OF CARE

Staff members are to endeavour to make each electronic communication truthful and accurate. They should use the same care in drafting e-mail and other electronic documents as they would for any other written communication. They are to keep in mind that anything created or stored on the computer system may be reviewed by others.

8.3 PROHIBITED ACTIVITIES

Inappropriate or unlawful material. Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate may not be sent by e-mail or other form of electronic communication (such as bulletin board systems, newsgroups, chat groups) or displayed on or stored in school computers or the Computer Resources. Users encountering or receiving this kind or material are to immediately report the incident to the Superintendent.

8.4 PROHIBITED USES

MECCS Computer Resources may not be used for dissemination or storage of commercial or personal advertisement, solicitations, promotions, destructive programs (that is, viruses or self-replicating code), political material or any other unauthorized use.

8.5 WASTE OF COMPUTER RESOURCES

Users may not deliberately perform acts that waste Computer Resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailing or chain letters, spending excessive or inappropriate amounts of time on the Internet, playing games, engaging in online chat groups, printing multiple copies of documents, or otherwise creating unnecessary network

traffic. Because audio, video, and picture files require significant storage space, files of this sort may not be downloaded unless they are business-related.

8.6 MISUSE OF SOFTWARE

Users may not do any of the following:

8.6.1 Copy software for use on their home computers unless proper authorization is given by the Superintendent or designate;

8.6.2 Provide copies of software to any independent contractors or clients or students or any other third person, unless authorization is granted by the Superintendent or designate;

8.6.3 Modify, revise, transform, recast, or adapt any software;

8.6.4 Reverse-engineer, disassemble, or de-compile any software;

However, for educational purposes, Users may, with prior written authorization from the Superintendent or designate install software on any of MECCS workstations or servers.

Users who become aware of any misuse of software or violation of copyright law are to immediately report the incident to the Superintendent or designate.

8.7 PASSWORDS

Responsibility for passwords. Users are responsible for safeguarding their passwords for access to the computer system. Individual passwords are not to be printed, stored online, or given to others, unless the school grants exceptions in this regard. Users are responsible for all transactions made using their passwords. No User may access the computer system or computer resources with another User's password or account, save the computer systems' administrators.

Passwords do not imply privacy. Use of passwords to gain access to the computer system or to encode particular files or messages does not imply that Users have an expectation of privacy in the material they create or receive on the computer system or the Computer Resources. The school has global passwords that permit it access to all material stored on its computer system regardless of whether that material has been encoded with a particular User's password.

8.8 SECURITY

Accessing other User's files. Users may not alter or copy a file belonging to another User without first obtaining permission from the User who made the file. Ability to read, alter, or copy a file of another User does not imply permission to read, alter, or copy that file. Users may not use the computer system to "snoop" or pry into the affairs of other Users by unnecessarily and inappropriately reviewing those files and e-mail.

Accessing other computers and networks. A User's ability to connect to other computer systems through the network or by a modem does not imply a right to connect to those systems or to make use of those systems unless specifically

authorized by the operators of those systems, except the users permitted to so by the Superintendent in the execution of their duties.

8.9 VIRUSES

Virus detection. Viruses can cause substantial damage to computer systems. Each User is responsible for taking reasonable precautions to ensure he or she does not introduce viruses into the MECCS network. To that end, all material received on disk or other magnetic or optical medium and all material downloaded from the Internet or from computers or networks that do not belong to the school are to be scanned for viruses and other destructive programs before being placed onto the computer system. Users must understand that their home computers and laptops may contain viruses. All disks transferred from these computers to the MECCS network is to be scanned for viruses.

Accessing the Internet. To ensure security and avoid the spread of viruses, Users accessing the Internet through a computer attached to the school's network must do so through an approved Internet firewall. Accessing the Internet directly, by modem, is strictly prohibited unless the computer you are using is not connected to the school's network.

8.10 ENCRYPTION SOFTWARE

Users may not install or use encryption software on any MECCS computers without first obtaining written permission from their supervisors or, relative to students, from the Superintendent. Users may not use passwords or encryption keys that are unknown to the Superintendent and/or the Computer Technician.

8.111 VIRTUAL FIELD TRIPS

The information networks offer many opportunities for "virtual field trips" to distant locations. MECCS considers all connections to remote locations as field trips. The rules that apply to student conduct on school-related field trips apply to these virtual electronic field trips as well. It is important that students realize that they represent their school when they use the information networks and that they must be on their best behaviour.

8.12 PLAGIARISM

Plagiarism is "taking ideas or writings from another person and offering them as your own." Credit must always be given to the person who created the article or the idea. The student who misleads readers to believe that what they are reading is the student's original work is guilty of plagiarism.

8.13 REPORTING OF INAPPROPRIATE INTERNET SITES

Anyone who becomes aware of an inappropriate Internet site is encouraged to advise the Superintendent of this so that appropriate steps may be taken to block the site.

8.14 MISCELLANEOUS

Compliance with applicable laws and licenses. In their use of Computer Resources, Users must comply with all software licenses; copyrights; and all federal, provincial, municipal and international laws governing intellectual property and online activities.

Amendments and revisions. This administrative procedure may be amended or revised from time to time as the need arises. Users will be provided with copies of all amendments and revisions.

9. MECCS will attempt to make every effort to ensure that this education resource is used responsibly by the Users. MECCS cannot, however, guarantee that unauthorized or inappropriate sites will not be accessed.

10. Administrators, teachers, and support staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to value and use the information to meet their education goals.

11. Students and staff have the responsibility to respect and protect the rights of every other User in the school and on the Internet.

12. Only the User authorized to access a network account will use it, subject to permission being granted by the Superintendent or designate. All Users must use the Computer Resources for its authorized purposes.

13. Students and staff are expected to act in a responsible, ethical, and legal manner in accordance with accepted rule of network etiquette, school policies and federal, provincial, and municipal laws.

14. The Principal (or the person to whom the Principal reports or his/her designate) shall have the authority to determine what is inappropriate computer or Computer Resource use by a User. He/she will note, in particular, that the following uses (but not just limited to the following uses) are prohibited: (The Principal or the person to whom the Principal reports may refer to procedure 16 as to other examples of inappropriate computer or Computer Resource use.)

    14.1 Use of the network or Computer Resources to facilitate illegal activity;

    14.2 Use of the network or Computer Resources for commercial or for profit purposes.

    14.3 Use of the network or Computer Resources for hate mail, discriminatory remarks, and offensive or inflammatory communication and material;

    14.4 Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.

    14.5 Use of the network or Computer Resources to access age-inappropriate sites.

    14.6 Use of inappropriate language or profanity on the network.

14.7 Use of the network or Computer Resources to create cyber-identities, to impersonate another, or the use of pseudonyms. Users must identify themselves honestly and accurately when participating in chat groups (if this is allowed), making posting to newsgroups (if this is allowed), sending e-mail, or otherwise communicating online.

14.8 Use of the network or Computer Resources to intentionally obtain or modify files, passwords, and data used by other Users, or disrupt the work of others.

14.9 Use of network facilities or Computer Resources for fraudulent copying, communications, or modification of materials in violation of copyright laws.

14.10 Downloading or installing games, programs, files, or other electronic media without the prior authorization of school staff.

14.11 Destruction, modification, or abuse of network hardware and software.

14.12 Quoting or forwarding personal communications without the original author's prior consent.

15. System security will be protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or school files. To protect the integrity of the system, the following procedures shall be followed:

    15.1 Users shall not ever reveal their passwords to another individual.

    15.2 Users shall not use a computer that has been logged in under another person's name.

    15.3 Any User identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

16. The school, acting reasonably and prudently, will protect users of the network and the Computer Resources, from harassment or unwanted/unsolicited communications pursuant to human rights legislation or other legislation. All Users who receive threatening or unwelcome communications shall immediately bring them to the attention of a teacher or an administrator. The teacher will report this information to his/her Principal. If the teacher and/or administrator is not sure whether this information can be shared in accordance with the *Freedom of Information and Protection of Privacy Act*, he/she is to discuss this with the Superintendent (FOIPP officer).

17. Student Users shall not reveal personal addresses or telephone numbers to other Users, or to other individuals, groups, organizations, and companies on the Internet.

18. The Principal has the authority to determine the appropriate level of supervision for Internet usage at the school in conformity of this policy.

19. Early in the school year, the Principal shall inform parents of the school's network and the procedures governing its use (see Administrative Procedure 140 Letter to Parents). Parents shall have the option of requesting that their child not be provided with privilege to access the Internet, the network, or the Computer Resources, while at school.

20. If the information to be shared by a User is a record under the *Freedom of Information and Protection of Privacy Act,* or is of a confidential nature, that information must not be shared through the network or the Computer Resources.

21. SANCTIONS

    Sanctions are at the discretion of the school and/or senior administrators based on the circumstances and the gravity of the violation.

References: Section 12, 60, 61, 113, *School Act*
Freedom of Information and Protection of Privacy Act
Canadian Charter of Rights and Freedoms
Canadian Criminal Code
Copyright Act
A.T.A. *Code of Professional Conduct*

Adopted: June 2011
Amended:
Due for Review: