TECHNOLOGY AND THE USE OF TECHNOLOGY

1. Purpose

This administrative procedure describes access to technology and sets out rules of conduct for technology and Internet use in the Medicine Hat Catholic Board of Education.

The use of technology in schools is intended to enhance the learning of students. It is intended that the use of computers and Internet access will provide connections to world-wide resources and facilitate local, regional and world-wide communications. The purpose of the Division's Internet access and other technological resources is to support and enhance learning and teaching by providing students and staff with the tools necessary to participate in the type of educational activities which will both prepare students for entry into the increasingly complex environment they will enter in the workforce and will ensure that teachers and other staff have access to the latest research materials. The network hardware and software is the property of the Division. The use of the network is a privilege and inappropriate use will result in a cancellation of those privileges.

The Division believes that the use of technology in schools will enhance the teaching/learning experience. The Division will continue to plan for the in-servicing of staff and the instruction of students in order to follow the program of instruction and meet the expectations of the learning outcomes for the use of technology. The Division is committed to ensuring equity of technological resources amongst the Division's schools.

2. Definitions

Network— A collection of computers and other hardware components interconnected by communication channels that allow sharing of resources and information. This includes Division local and wide area networks, as well as external regional and global networks.

Technology – Division and personal computer hardware and software, peripherals, devices and other technological tools used to support instruction, administration and operations.

User— Any student, employee, Board member, volunteer, or community member or group who uses technology (as defined above) or Internet services.

3. Internet Use for Education Purposes

3.1 Students in the Medicine Hat Catholic Board of Education have access to the Internet for educational purposes. Educating students on the effective use of the Internet provides access to a vast amount of learning material. Providing age appropriate Internet filtering helps to protect against access to inappropriate material. Every effort to provide a safe learning environment will be made, however, due to the changing nature of the Internet, users may inadvertently obtain access to information that may be considered to be inappropriate, obscene, abusive, offensive, harassing, illegal, or to counsel illegal activities.

4. Procedures

4.1 The Director of Information Systems will coordinate and maintain the provision of network and Internet access within schools and administrative buildings.

4.2 The principal or designate is responsible to ensure that users obey the Rules of Conduct defined in Section 5: Rules of Conduct.

4.3 Supervisors, including principals, shall consult with the Superintendent of Schools if they have questions about appropriate technology or Internet use not covered in this procedure.

4.4 Penalties for not adhering to these procedures may include temporary or permanent withdrawal of the user's technology and Internet privileges, payments for damages or repairs, discipline under appropriate Division procedure including suspension, expulsion, exclusion or termination of employment, and civil or criminal liability under applicable laws.

4.5 Upon registration at school, parents/guardians, or the student, if over age 18, will be informed that the learning environment may include access to Internet resources

5. Rules of Conduct

A network account will be provided to each user. The following Rules of Conduct apply to each user.

5.1 It is a privilege to use technology, as defined in this procedure, and to have a network account.

5.2 The user is responsible for his/her network account and for any use made of that account. The user must not allow another person to use his/her account under any circumstances.

5.3 The user must keep his/her password confidential and will report to his/her teacher, supervisor or school principal if he/she suspects another person has access to his/her network account.

5.4 The user will access the network only for district sponsored educational and administrative purposes which may include but not be limited to academic exchanges, special projects, support services, curriculum, and professional development activities.

5.5 The user is responsible for the information sent electronically from his/her account whether sent as private email, public posting, or on the World Wide Web, and must meet the standards for any similar, non-electronic communication.

5.6 The user will not engage in any activity which undermines the operation of the network, including but not restricted to the following:

5.6.1 interference with the functioning of a school network, the district connection, or any other network that can be accessed through the Internet;

5.6.2 causing a disruption in any services available through the network or Internet;

5.6.3 the use of unlicensed software and/or use of licensed software in excess of licensing agreements;

5.6.4 using the computer system while access privileges are suspended or revoked;

5.6.5 attempting to gain unauthorized access to any computer system, network, data, resources, programs, or system privileges;

5.6.6 attempting to find or exploit any gaps in system security on a school network and the district network. If the user notices any other weaknesses or suspects anyone of tampering with system security, the user must notify the teacher, principal or supervisor immediately.

5.6.7 using his/her account or the network to access, create or distribute information (video, audio, images, text, etc.) which is obscene, harassing, threatening, racist, inflammatory, malicious, fraudulent, libelous or unprofessional. The user's account will not be used for any activity that may be considered unethical, immoral, or illegal.

5.6.8 decrypting (decoding) any encrypted material for which the user does not have authorization; and

5.6.9 intentionally seeking information about, browsing, obtaining copies of or modifying files, passwords or data belonging to other people, regardless of the location.

5.7 The Superintendent of Schools, or designate, reserves the right to suspend or remove the user's account if the user contravenes these Rules of Conduct.

6. Appropriate Use

6.1 The Superintendent of Schools, or designate, reserves the right to filter unsolicited email (spam) and Internet sites deemed inappropriate.

6.2 Every effort will be made to host electronic information on district servers and school/district sponsored collaborative learning environments (Twitter school\class account, YouTube school\class channel, etc.) with consideration for staff and student privacy. Schools that are considering using external collaborative learning environments need to consult with the Superintendent of Schools prior to proceeding. All electronic information hosted in these learning environments would be subject to Section 5: Rules of Conduct.

6.3 Email links for employees or students must point to district email accounts only. District accounts should be used for educational and work related use. Personal use should be directed to personal accounts

6.4 The Division retains ownership and possessory control of its computers, hardware and software at all times. To maintain system integrity, monitor network etiquette, and ensure that users are using the system responsibly; the Superintendent of Schools or designate may review user files and communications. Users shall not expect that files and other information communicated or stored on Division servers will always be private.

6.5 When using a Division Device such as a cellular phone, smartphone, Telco enabled tablet, data stick, or any other Device that is bound by a subscription or contract with a third party, it is the responsibility of the user to ensure appropriate use in an effort to reasonably maintain usage charges. In addition, should you be required to use a Division Device outside of your normal area that requires your device to “Roam”, it is the user’s responsibility to contact the Director of Information Systems, or designate, to ensure that the Network usage subscription or contract reasonably maintains usage charges. Failure to maintain reasonable usage charges day-to-day or while travelling may result in re-imbursement payment for excessive use.

6.6 Employees are discouraged from excessive use of the Division’s e-mail, voice mail, mobile phones and computer systems for personal use.

7. Use of Classroom Resource Mobile Devices

7.1 Classrooms may be provided with technology in the form of mobile devices. These devices offer portability of use by employees and students for work- and school-related activities. Additional care and understanding of how the devices should be handled, used and stored is required

7.2 The following pertains to the use and safekeeping of classroom resource mobile devices by students or employees:

7.2.1 No personal or confidential information should be stored on these devices.

7.2.2 Any files saves to this device should be transferred to a district network storage area while logged in at school or work. The device is not backed up, whereas network storage is backed up regularly.

7.2.3 Software on the device will be updated throughout the year. Schools will be given advance notice of this occurring.

7.2.4 The device will be used by students and employees. Information and Technology Services has implemented security functionality on devices that need authentication to isolate users from one another. Even so, each user must remember that the device will be shared.

7.2.5 As a portable unit, the device is more susceptible to theft. Therefore, additional care must be taken to safeguard the device to prevent an information breach.

7.3 Classroom resource mobile devices are property of the Medicine Hat Catholic Board of Education and do not belong to any one individual.

7.4 Classroom resource mobile devices that are intended for use outside the school setting, such as taken home by an employee to do report cards or used during a school sponsored event. While outside the school setting these devices are to be used only by the specific employee or student with the permission of the teacher.

7.5 Only school or district-approved software/applications are to be installed. Personal software licensed is not permitted.

7.6 Any damage or loss that occurs to a classroom resource mobile device that has been removed from a school is the responsibility of the school. This includes making changes to the device that renders it inoperable.

7.7 If a mobile device goes missing, the user must notify the principal immediately in order to activate breach procedures.

7.8 Classroom resource mobile devices have a finite battery life. Planning for charging and access to an AC power outlet must be considered. Charging routines should be established for consistent use.

7.9 Where at all possible, classroom resource mobile devices should be stored in a secure location when not in use.

7.10 Due to the size, shape and weight of classroom resource mobile devices, the device must be handled with care. Attention is required when packing, transporting and using them.

7.11 Wireless networks are widely available within and outside the school. Users who connect to multiple wireless networks must take care to ensure that MHCBE wireless network information is not removed.

8. Use of Personally Owned Devices

The Medicine Hat Catholic Board of Education will permit Personal Devices to access the District Network. The following Rules of Conduct apply to each user,

8.1 The cost of acquiring and maintaining the Personal Device as well as all operational/connectivity charges are the responsibility of the user. The Division may choose to provide employees with a connectivity/usage allowance as appropriate to their roles and/or responsibilities. In addition, the Division shall not be responsible for any increased or additional connectivity charges incurred by the employee as a result of accessing the Division Network with a Personal Device over and above the assigned allowance. Under special circumstances when a Personal Device is required when travelling and this results in higher than normal Network usage charges, these may be claimed by normal expense process.

8.2 By receiving access to the Division Network the user grants to the Division the right to access the Device with or without notice to investigate, review, delete, remote wipe Division Data, and/or remote kill and disable the Device at any time for any reason. The Division will not be liable for the loss of any Personal data arising from such actions by the Division.

8.3 When syncing and/or connecting a personal device to the Division Network the user must ensure that any remotely retrieved and stored Division Data be protected and treated as private. The Division will enforce a strict password policy on remote devices that sync and/or connect to the Division Network by requiring a device password in order to access and connect to the Division Network.

8.4 If the Division suspects a security breach related to a Personal Device it may, with or without notice, take any and all actions deemed appropriate to secure the Division data and the Division Network, including, but not limited to, disconnecting the Device from the network and remote wiping Division data and/or killing or disabling the Device.

8.5 By receiving access to the Division Network with a Personal Device, the users agrees to be subject to and comply with all applicable Division rules, regulations, and policies, including the security and other usage guidelines set forth in Administrative Policy 140.

9. Protecting Personal Privacy

9.1 The use of technology, including devices with digital imagery and cellular capability, must be used in an appropriate manner that respects the privacy and dignity of others. Such technology must not be used in areas where there is an expectation of privacy, such as in washrooms or change rooms.

9.2 Unless it is a school-sanctioned activity, users must not take photographs, videos or audio recordings of a person or persons on school property, at school events/activities during school hours unless prior approval of the person(s) and principal or designate has been received in writing.

9.3 Failure to obey Section 9: Protecting Personal Privacy will be dealt with according to school procedures, administrative procedures and/or the police protocol.

10. Loss, Damage, or Theft of Personal Electronic Devices

10.1 Students and employees are responsible for safe-keeping their personal electronic devices. The school or administrative office is not responsible in the event of loss, damage or theft.

10.2 If a student fails to abide by the rules of conduct outlined in this procedure, the electronic device may be confiscated and returned to the parent or guardian, or to an adult student after the instructional day, or as appropriate to the circumstances.

11. Security Breach of Digital Information Checklist

11.1 As soon as a user suspects a breach of digital information, the user must immediately notify by email, the Director of Information Systems.

11.2 The user will report in an email to the Director of Information Systems, all known information about the possible breach of digital information.

11.3 If the user is in a school setting a copy of the notification e-mail will be sent to their building Principal. If the user works in central office the user will send a copy of the e-mail to their immediate supervisor.

11.4 Upon receipt of a notification e-mail concerning a suspected breach of digital information the Director of Information Systems will immediately notify the Superintendent of Schools and the Division's FOIP Officer. The Director of Information System will also send an e-mail to the person reporting the suspected breach of digital information confirming that the notification has been received.

11.5 Upon receipt of a notification e-mail concerning a suspected break of digital information the Director of Information Systems will immediately launch an investigation and within 12 to 24 hours make initial recommendations to the Superintendent of Schools.

12. Digital File Transfer

12.1 From time to time employees in the Division move from one school to another. As a result of this movement employee digital files must also be transferred as

required. It is the responsibility of the Division that this transfer is completed in a way that does not expose the content of those files to unauthorized users.

12.2 All digital file transfers for employees will only be completed once the Information Technology Department receives a Staffing Notification from Human Resources. Information Technology will designate one staff member who will be responsible for digital transfers. Once the designated employee has completed the transfer he/she will confirm the action on the staffing notification form and place the document in a file. Should there be problems with the transfer of data, the issue will be discussed by the designated employee and the Director of Information Systems before any further action is undertaken to ensure the file has not been mistakenly placed.

13. Disclaimer

13.1 Every effort will be made to ensure the privacy of a user's information. However, all information that is sent, received and created using the district network is subject to examination, if deemed appropriate, by the Superintendent of Schools or designate.

13.2 The Medicine Hat Catholic Board of Education does not accept any responsibility for the use or misuse of information acquired by any user accessing the Internet using technology, as defined in this procedure, nor any situations, issues or litigation that may arise from unauthorized use or contravention of any of Section 5: Rules of Conduct.

Reference: 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