

130 RESPONSIBLE USE OF TECHNOLOGY

Beliefs

The Maskwacis Education Schools Commission (MESC) follows cultural and traditional teachings of the Maskwacis Cree, in particular Wahkohtowin. Wahkohtowin is the belief that all things are related and connected, that all of existence has spirit and that living in a good way requires us to maintain good relationships with each other and other aspects of existence. We recognize that respect for mother earth, elders, youth, and the Treaties are paramount to planning ahead and making decisions for future generations.

MESC encourages the use of computer technology and networks to enhance teaching and learning, and to support administrative functions.

Procedures

1. Use of the network and the Internet must be in support of, and consistent with, the educational objectives of MESC and must conform to Board policy and administrative procedures.
2. Students and staff will be provided with individualized accounts and passwords to access computer and online services.
3. Do not use @maskwacised.ca email addresses to sign up for any online site not authorized by MESC and approved by MESC IT.
4. Do not use the same password attached to your MESC email with any online site authorized by MESC and approved by MESC IT.
5. MESC technology must be used in ways that are consistent with the following principles.
 - 5.1. Appropriate Use
MESC technology is intended for educational purposes and for business activities in the operation of schools and MESC. Personal use of electronic communication must not interfere or conflict with its use for work purposes. MESC technology shall be used for purposes that are legal, ethical and moral.
 - 5.2. Privacy and Personal Safety
Activities involving MESC technology will, as much as possible, protect the privacy of personal information of all users and the personal safety of students. All users will be educated about ways that they can protect their own personal information and personal safety.
 - 5.3. Security of Systems and Information
Individuals using MESC technology shall not compromise the security and integrity of data and information stored on MESC or school computer systems.
6. Students will be given access to MESC technology for educational purposes that include:
 - 6.1. Achieving the learner outcomes.

- 6.2. Participating in learning activities selected by the teacher/instructor.
 - 6.3. Participating in online MESC programs.
- 7. Staff will be given access to MESC technology for purposes that include:
 - 7.1. Communication.
 - 7.2. Information acquisition.
 - 7.3. Information management
 - 7.4. Professional development and training.
 - 7.5. Providing technology support to other users of MESC technology.
 - 8. Volunteers may be given access to MESC technology for purposes that include:
 - 8.1. Communication.
 - 8.2. Information acquisition.
 - 8.3. Assisting staff in using MESC technology with students.
 - 9. Students and their parents/caregivers will sign an Acceptable Use of Technology Agreement that confirms their understanding of MESC expectations and procedure as part of the registration process.
 - 10. All users will be responsible and accountable for their use of MESC technology.
 - 11. Students who deliberately use MESC technology inappropriately will be subject to some or all of the consequences:
 - 11.1. Loss of computer and network privileges.
 - 11.2. Suspension.
 - 11.3. Legal action.
 - 12. Staff who deliberately use MESC technology inappropriately will be subject to disciplinary or legal action, which may include termination of employment.
 - 13. Other users who deliberately use MESC technology inappropriately will lose the privilege of using MESC technology.
 - 14. Unacceptable use of the network includes, but is not limited to:
 - 14.1. Using the network for any illegal activity, including violation of copyright laws.
 - 14.2. Using the network in ways which violate policies, administrative procedures, and behavior standards.
 - 14.3. Using the network for financial or commercial gain.
 - 14.4. Degrading or disrupting equipment or system performance.
 - 14.5. Invading the privacy of other individuals by accessing and/or vandalizing their electronic data.
 - 14.6. Wasting technology resources, including bandwidth, file space, and printers.
 - 14.7. Gaining unauthorized access to resources or entities.
 - 14.8. Using an account owned by another user, with or without their permission.
 - 14.9. Posting personal communication without the author's consent.
 - 14.10. Any activity that could compromise an individual's position as a representative of MESC.

15. Protecting Information: Accounts and Passwords
 - 15.1. Do not reveal your or any other person's personal information (e.g., home address, telephone number, passwords, etc).
 - 15.2. Do not reveal any passwords assigned to you.
 - 15.3. Do not share your password with any other person
 - 15.4. If you think your account or password might be compromised, please report it to the IT Service Desk right away
 - 15.5. Do not write down or store passwords unencrypted.
16. Network Etiquette
 - 16.1. Use good judgment and communicate in a respectful manner.
 - 16.2. Report any threatening or inappropriate material to a teacher or administrator.
 - 16.3. Do not send spam, chain letters, or other mass unsolicited emails.
 - 16.4. Do not engage in activities prohibited under municipal, provincial or federal law.
 - 16.5. Do not video, audio record, or take photographs of others and upload them without permission.
 - 16.6. Electronic mail (e.g., e-mail) is not private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities will be reported to the authorities and will result in the loss of user privileges, and other appropriate disciplinary actions.
 - 16.7. Use the network and Internet in such a way that you will not disrupt the use of the network by other users.
 - 16.8. All communications and information accessible via the Internet should be assumed to be the private property of those who put it on the network.
 - 16.9. If you see a security problem on the network, report it to a system administrator.
17. Use and Installation of Software
 - 17.1. Only individuals designated by a school or site administrator shall be authorized to install software on MESC computer technology.
 - 17.2. No one shall install illegal or pirated software on any computer.
18. Filters will be used to block access to inappropriate sites and MESC network. Site administrators may grant limited access to some sites for educational or business purposes. Users may, however, encounter material that is controversial, inappropriate, or unacceptable. It is the user's responsibility not to initiate access to such material and to cease access to such material immediately. Such material must be reported to a staff member immediately, who will in turn report the matter to infosec@maskwacised.ca.
19. MESC shall not be liable for any decision by any service provider or by MESC itself to restrict access to or to regulate access to material on the Internet. MESC does not control material on the Internet and is therefore unable to control the content of data that a user may discover or encounter through use of the Internet.

20. MESC may monitor the use of technology on a periodic basis checking for breaches of security, violations of law, or infringement of MESC rules, Board policy or administrative procedures. Such monitoring may occur electronically or manually and without prior notification.
21. All Staff that have been provided with a portable technology are responsible for their storage so that the risk of a stolen or lost device is minimized.
22. Personal Communication Devices (PCDs) are not to be operated by students during regularly scheduled instructional time, or during any school sponsored activity, such as an assembly or talk by a guest speaker, unless such use is approved by the classroom teacher to facilitate learning activities.
 - 22.1. PCDs using the school's wireless network can be monitored and activities can be traced back to the student.
 - 22.2. PCDs are not to be taken into test or examination settings, unless students have been given permission to do so.
 - 22.3. PCDs are not to be used in settings such as change rooms, washrooms, private counselling rooms, that have the potential to violate a person's reasonable expectation of privacy.
 - 22.4. PCDs are valuable electronic devices. The security and storage of these items is the sole responsibility of the owner/user. The MESC assumes no responsibility for the safety, security, loss, repair or replacement of PCDs.
 - 22.5. Technical support for PCDs is the responsibility of the student and not MESC personnel.
 - 22.6. PCDs which are taken temporarily from students by teachers or administrators must be securely stored and returned to the student or his/her Parent/Guardian/Caregiver, as appropriate, on the same day or at the time agreed upon with parent/guardian.

Reference:

Personal Information Protection Act
Canadian Charter of Rights and Freedoms
Canadian Criminal Code

Appendix A:

Student School Engage Registration Form: Acceptable Use of Technology Agreement for Students

Maskwacis Education Schools Commission (MESC) recognizes the educational value of technology in our schools and classrooms. Students benefit from the access, use and shared educational information obtained from the Internet, including access to online school resources, collaboration opportunities and personalized learning. MESC provides a Wide Area Network that connects our facilities and permits access to the Internet for students and staff. MESC provided technology is used to enhance teaching and learning, increase student success, and help students become responsible digital citizens.

In this agreement, technology includes, but is not limited to, desktop/laptop computers, iPads/tablets, Chromebooks, Internet access, G Suite for Education accounts from Google, software, digital cameras, printers, interactive displays, televisions, and any new or emerging technology. This agreement will be used to support teaching and learning and to establish a shared understanding of the acceptable use of technology in schools across MESC.

Conditions and Rules for Use

MESC network administrators and their authorized employees monitor the use of network and technology resources, including G Suite accounts, to help ensure that users abide by this agreement. The use of MESC's network system and technology is a privilege and should be respected as such, MESC retains the right to limit, suspend or restrict access to the MESC network systems and technology.

1. Acceptable Use

- Students may use technology for educational purposes only.
- Students may only download, save, or install software, music, movies, and images if instructed by their teacher, and in accordance with MESC Copyright policy (Admin Procedure 134), and copyright laws.
- Students will handle all technology hardware with care and respect.
- Students will use technology for legal activities and educational purposes only.
- Students will use technology in compliance with school standards and MESC Student Conduct policy (Admin Procedure 307).

2. G Suite Applications

- By signing this agreement, parents/guardians and students are providing informed consent for the creation and use of the student's MESC G Suite account.
- MESC provides its students access to Google's *G Suite for Education* Core Services (i.e. Calendar, Classroom, Drive and Docs, Gmail, Keep, Tasks, etc.) to enhance learning and student success.
- Students may also be given access to *G Suite for Education* Additional Services as learning tools.
- According to Google's Terms of Use, students under the age of 13 will not have access to Youtube through their MESC account.
- Google's data is primarily stored in the US and therefore the data is subject to US laws. The *G Suite for Education* Agreement between MESC and Google provides assurances that Google will not release any personal information unless it is required to do so by law, and only after they have made reasonable efforts to notify the user of the request and provide MESC with a chance to challenge the disclosure.

3. Network Etiquette

Students are expected to honour Wāhkōhtowin and abide by the generally accepted rules of network etiquette and digital citizenship. These include, but are not limited to:

- Use good judgement and communicate in a respectful manner.
- Report any threatening or inappropriate material to a teacher or administrator.
- Do not send spam, chain letters or other mass unsolicited emails.
- Do not video, audio record or take photographs of others or upload them to the Internet.
- Do not share or disclose personal information about yourself or others, including age, address, schedule of activities, and phone numbers.
- Respecting copyright by quoting and citing of any information from the Internet.
- Only use the assigned MESC network and G Suite account, and keep this information confidential.
- Do not use an account owned by other users; do not share your passwords.

4. Personally-Owned Devices

Schools determine if students can utilize their personally-owned devices at school, and if permitted, students may be given access to the MESC wireless network. If students use personally-owned devices on MESC property, all of the above conditions apply, as well as the following:

- Personally-owned devices using the school's wireless network can be monitored and activities can be traced back to the student.
- Students will use personally owned devices only when given the teacher's expressed permission.
- Technical support for personally-owned devices is the responsibility of the student and not MESC personnel.
- The school is not responsible for the loss, theft or damage of personally-owned devices.

- MESC personnel may be granted access to the student's personally-owned device if there are reasonable grounds to believe that the device has been involved in a breach of school policy or MESC Student Conduct policy (Admin Procedure 307) and that an investigation of the device may reveal evidence of the breach. Evidence may include, but are not limited to, audio and video recordings or photos that violate the privacy of others, vandalism, harassment, bullying and immoral or illegal activities. The disclosure of such evidence may lead to disciplinary or legal action.

I have reviewed and discussed the Acceptable Use of Technology Agreement with my student, and by signing below, I agree that they will follow the rules and expectations outlined in this agreement.

This field is required.

Parent Name/Signature