SIMCOE MUSKOKA CATHOLIC
DISTRICT SCHOOL BOARD

Learning Environment

Policy Number LE-25

Responsible Use of Information and Communication Technology (ICT)

It is the policy of the Simcoe Muskoka Catholic District School Board (SMCDSB) to provide and maintain access to information and communication technology for use by students, SMCDSB staff and other users in a manner which is consistent with the Ontario Catholic School Graduate Expectations, SMCDSB's strategic plan, mission and vision statements, Catholic virtues and values, Ministry of Education guidelines and with all federal, provincial and municipal laws and regulations.

Legislation

The Education Act, R.S.O. 1990, C. E.2
The Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M.56
The Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sched. A
The Personal Information Protection and Electronic Documents Act, S.C. 2000, c.5
Canada's Anti-Spam Legislation s.c. 2010, c. 23

Procedural Guidelines Follow

Responsible Use of Information and Communications Technology (ICT)

Approved: Board Meeting #16-2013 (Wednesday, November 27, 2013)
Revised: Board Meeting #6-2018 (Wednesday, April 25, 2018)
Revised: Board Policy Review Meeting #04-2022 (Wednesday May 11, 2022)
Revised: Board Meeting #08 (Wednesday, June 15, 2022)

Procedures and Guidelines Supporting Policy Number LE-25
Responsible Use of Information and Communication Technology (ICT)

Responsible Use Procedure for Information and Communication Technology (ICT) for Students and Staff

1. This document outlines the expectations related to the responsible use of information and communication technology (ICT) and its associated resources, including hardware, software, network, Internet usage and social media. It is reasonable to expect that all individuals or groups who use SMCDSB's technology understand and comply with the expectations outlined in this procedure.

2. Students will be required to review age appropriate information related to this policy, with a focus on digital citizenship, responsibilities and consequences. Parents and students are required to read and sign a Responsible Use of Technology Agreement annually.

3. Staff and SMCDSB Trustees are expected to read and understand Policy LE-25 and the supporting procedures and guidelines. All new staff must complete a module in the online staff training portal related to the responsible use of ICT. Each year, staff will be required to complete a responsible use of ICT refresher via the online staff training portal. This refresher requires staff to review and agree to policy LE-25 and its supporting procedures and guidelines.

4. Other members of the school community including visitors and volunteers are expected to understand and adhere to this policy and its supporting procedures and guidelines when accessing SMCDSB ICT.

5. **Electronic Monitoring**

   Users must recognize the system is provisioned by SMCDSB for work and educational purposes that give it a strong interest in having access to accounts and information. A list of our systems and what is monitored is provided in Appendix A.

   a. To that end SMCDSB conducts electronic monitoring for the following reasons and in the following circumstances:
      i. Performing System maintenance and repair;
      ii. Protecting staff, students and technology from harm;
      iii. Investigating System misuse;

- iv. Proactively monitoring and auditing for System misuse;
- v. Complying with a legal obligation;
- vi. Supporting work continuity; and
- vii. Conducting research.

b. Routine Monitoring: SMCDSB routinely monitors electronic systems and may monitor and access any file, document, electronic communication and use of the internet at any time to ensure the integrity of our electronic systems.

c. Demand Monitoring: SMCDSB maintains the right to access data collected via our electronic systems (Board provided technology or personal devices when using Board credentials and/or networks) may arise in a number of situations, including but not limited to:

- i. To comply with legislative disclosure or access requirements under MFIPPA (Municipal Freedom of Information and Protection of Privacy Act) and PHIPA (Personal Health Information Protection Act) or to assist with the investigation and resolution of a Privacy Breach. (Requested by Research, Information and Privacy Officer and approved by the Director of Education);
- ii. For Board owned technology, because of regular or special maintenance of the electronic information systems (Requested by authorized IT Staff and Approved by Senior Manager ICT Service);
- iii. For Board owned technology, when the Board has a business-related need to access the employee’s system, including, for example, when the employee is absent from work or otherwise unavailable (Requested by Supervisor and Approved by Senior Manager ICT Service);
- iv. To comply with obligations to disclose relevant information in the course of a legal matter (Requested by the Executive Human Resource Officer or Supervisory Officer and approved by the Director of Education or Superintendent of Policy, Finance and Business Services);
- v. When the Board has reason to believe that there has been a violation of the Code of Conduct, Board Policy, or is undertaking an administrative, legal or disciplinary investigation (Requested by Authorized Executive Human Resource Officer and Approved by a member of ELC.);
- vi. For Video Surveillance, as outlined in GP-18 - Video Surveillance.

SMCDSB may, in its discretion, use information obtained through electronic monitoring to determine if there has been a violation of its policies. Where appropriate, such information may lead to disciplinary action, up to and including termination of employment, including for cause.

This updated Administrative Procedure seeks to meet the requirements put in place by recent legislative amendments added to the Employment Standards Act, 2000 (ESA) on April 11, 2022. Nothing in this Administrative Procedure shall be interpreted to create any greater right or benefit than what is available under existing legislation, or to restrict any of the Board's legal rights. A copy of the updated procedure will be provided to each employee within 30 days of the date of revision being made. All new employees will be provided a copy of LE-25 Responsible Use of ICT within 30 days of their start date.

6. **Digital Citizenship**

Definition: Digital citizenship outlines the norms of appropriate and responsible behaviour as it relates to technology use, including hardware, software, Internet usage and social media.

The *Ontario Catholic School Graduate Expectations* were designed by the Institute of Catholic education to guide school boards in their programming and work in Catholic education. One of the expectations is to be "responsible citizens who: act morally and legally as a person formed in Catholic traditions, accept accountability for their own actions and contribute to the common good." This particular expectation is a reference point for students and staff who are members of a digital community.

SMCDSB is committed to effective digital citizenship and expects the same of all students and staff. This includes creating a positive school and work culture which supports the safe and responsible use of ICT through the following areas:

a. **Access**
SMCDSB is committed to providing equitable access to ICT for students and staff. This includes:
   i. Accessing a variety of quality resources;
   ii. Accessing technology when and where the learning occurs;
   iii. Providing adequate training and support on the effective use of ICT resources; and
   iv. Providing opportunities to collaborate and communicate with local, national and international communities.

b. **Communication and Relationships**
Connecting with one another from a distance or through a screen name, is very different from a face-to-face encounter. It is easier to behave irresponsibly, cruelly, or unethically and it is also common for others to misinterpret the tone and context of messages or posts.

SMCDSB expects students and staff to be mindful of their online exchanges. Always take time to recognize that different audiences require different types of communication and ensure words are chosen wisely.

c. **Literacy**

Through SMCDSB's ICT, students and staff have access to a wide range of tools and resources for learning. It is important for users to know that information found online is not always accurate or high-quality.

SMCDSB is committed to enhancing the digital literacy skills of its users by helping to identify the legitimacy of online sources and promoting strategic online searches.

d. **Etiquette and Appropriate Use**

Students and staff are responsible for appropriate behaviour when using SMCDSB's ICT resources just as they are in a classroom, a school, a work site, or SMCDSB sponsored activity. Appropriate use of ICT resources is outlined more specifically in the Responsibilities section below.

e. **Security and Privacy**

Security and privacy are important in the digital world. It is the responsibility of students and staff to treat SMCDSB's ICT with the same level of protection and respect they would with personal belongings. This means keeping digital security top of mind when using ICT resources, including backing up data, virus protection and maintaining the integrity of passwords.

In addition, as noted in 5.0 above users do not have a reasonable expectation of privacy when using SMCDSB ICT resources and are subject to the *Freedom of Information Protection of Privacy Act.* SMCDSB also has the right, but not the obligation to, inspect and/or monitor any ICT resources.

f. **Copyright**

Understanding and adhering to copyright laws are an important component of digital citizenship. In our digital culture we can gain access to information quickly and easily without fully understanding where the content comes from or to whom it belongs. It is important for students and staff to always consider, understand and adhere to copyright laws. This includes gaining permission to use copyrighted work and understanding that piracy and plagiarism are unethical and unlawful.

g. Creation, Collaboration and Communication

Technology allows users to learn, create, collaborate and communicate. Students and staff should be aware that all content including work plans, course binders, project documentation, electronic correspondence, presentations, artwork and any other documentation, which is completed (or in progress) for the purposes of a user's role at SMCDSB, are considered to be the intellectual property of SMCDSB.

7. Responsibilities

In order to ensure appropriate use of SMCDSB’s technology, including hardware, software, Internet usage and social media, students and staff are required to:

a. Use SMCDSB’s ICT resources, Internet and social media for educational purposes only;

b. Maintain the distinction and separation of those digital activities that are personal from those that are provided to support learning;

c. Teaching staff should not issue or accept friend requests or follow students on social media. An exception would be if a staff member has a classroom account where curricular information is shared with students, then students may follow that account. Staff should also consider the privacy implications of accepting these requests from parents;

d. Model appropriate behaviour as a digital citizen by using ICT resources in a moral, ethical and lawful manner;

e. Observe standards of academic honesty by never misrepresenting the work of another as an original work (plagiarism), acknowledge sources by using appropriate citation methods and obey all applicable copyright laws;

f. Receive appropriate approval prior to adding software, applications and social media accounts on ICT resources;

g. Always maintain the integrity of passwords. This means never disclosing your own passwords to anyone or attempting to access SMCDSB's technology with another person’s password. Each user shall be responsible for all activities arising from the use of their password. Users shall take reasonable precautions to protect the integrity of SMCDSB’s systems, including using adequately complex passwords;

h. Users are expected to maintain SMCDSB’s values and the integrity of its technology. For staff, there is also an expectation that student use of ICT resources are monitored/supervised appropriately.

i. Be aware and abide by the SMCDSB’s responsible use guidelines. Specific violations of these guidelines include:

    i. Using SMCDSB technology to create, process, distribute or access illegal, offensive, pornographic and/or inappropriate materials;

    ii. Sending/receiving defamatory, abusive, obscene, profane, sexually oriented, threatening or racially offensive messages;

    iii. Downloading or storing obscene or offensive material on SMCDSB ICT resources (computers, networks, social media);

    iv. Downloading, storing or sharing media files, including music and video files on SMCDSB computers, network, social media that are illegal, offensive, obscene, inappropriate or that are not intended for SMCDSB purposes;

    v. Knowingly accessing sites containing material contrary to the human rights code or clearly inappropriate in a SMCDSB environment, including sexually explicit, racist or defamatory material;

vi. Uses that are malicious, unethical or in violation of accepted community standards or SMCDSB policies;

vii. Uses that violate any federal or provincial laws, including the Ontario Human Rights Code;

viii. Knowingly creating, exchanging, transmitting and/or downloading messages or data that are offensive, harassing, obscene, libelous, abusive, discriminatory, or threatening or that encourage violence;

ix. Conducting business activities which are unrelated to the user's duties and responsibilities to SMCDSB;

x. Attempting to access another person's account or private files or misrepresenting yourself as another person in electronic communications;

xi. Sending anonymous or inappropriate, unsolicited mass email messages, such as chain letters, jokes or spam;

xii. Computer-hacking and malicious related activities, like phishing/ransomware; and

xiii. Attempting to disable or compromise the security of information contained on SMCDSB computer systems.

8. **Consequences**

SMCDSB has the right, but not the obligation to inspect and/or monitor any ICT resources and retains the right to deny access to anyone using SMCDSB provided resources, regardless of location, when used for a purpose other than the spirit and intention for which they are granted.

Based on this policy, school and board administrators and supervisors, with appropriate consultation, will decide whether technologies and/or services have been used appropriately. If deemed inappropriate or abuse of privilege, board administrators and supervisors will determine the consequences and discipline. These may include loss of technology privileges, and/or other consequences consistent with the Board Code of Conduct and policies and procedures.

Certain breaches of this policy may constitute an offence under Canada's Criminal Code and other applicable legislation. Where appropriate, offences of this nature will be reported to the appropriate authorities and dealt with accordingly.

a) **Student Disciplinary Action**
In the event that a student has violated this Responsible Use Agreement, the student (and the parent/guardian) will be provided with notice of such violation by the school principal and be given an opportunity to present an explanation. Disciplinary action will align with the violation and will be consistent with:

○ SMCDSB's Student Discipline Policy (Safe Schools); and

- The standards of behaviour as outlined in the Provincial Code of Conduct and the Board Code of Conduct, as they apply to all members of the school community including students, parents and guardians, all staff members, volunteers and visitors who access SMCDSB owned devices or network, while on SMCDSB property or to conduct SMCDSB related business.

Disciplinary action can include (but not be limited to):

- Restriction and/or denial of access to SMCDSB's networks;
- Contacting appropriate legal authorities if there is suspicion of illegal activities; and
- Consequences as outlined in the Board Code of Conduct, e.g., suspension or expulsion.

APPENDIX A TO ELECTRONIC MONITORING

Tool	What is monitored?	How	Purpose
Web filtering	All internet traffic	Network Management and monitoring tools	Protect from harmful and inappropriate content. Troubleshooting and support.
Electronic Communications	All Electronic Communications	Data Loss and Prevention tools, and Network Management tools	Prevent the transmission of inappropriate/confidential data over insecure e-mail. Troubleshooting and support.
Network Monitoring	All network traffic	Packet analysis	Protect the integrity and availability of the network. Monitor overall usage and protect against unauthorized access. Troubleshooting and support.
Account Authentication	Staff login to services	Authentication Services	Protect against unauthorized access. Troubleshooting and support.
Device Management (iPad/iPhone)	Installed on all Board iPads/iPhones	Mobile Device Management, and Endpoint Security Tools	Protect against loss/ theft and enforce security settings. Troubleshooting and support.
Device Management (Chromebook)	Installed on all Board Chromebooks	Management Console, and Endpoint Security Tools	Protect against loss/ theft and enforce security settings. Troubleshooting and support.
Device Management (laptop, Desktops)	Installed on all laptops and desktops	Mobile Device Management and Endpoint Security Tools	Protect against loss/ theft and enforce security settings. Troubleshooting and support.
Phone logs	Some facilities	Phone System	Call quality (e.g. bandwidth, latency, jitter, packet loss, compression), call volume and voicemail storage monitoring. Troubleshooting and support.
Video surveillance	Some facilities	Video surveillance cameras and recording systems	Safety, theft, illegal activity, behavioural/ incident monitoring and review. Controlling and monitor access to our Data Centre.
Access Badges/Fobs	All facilities	Through Door Reader	Control and monitor access to buildings. Administrative investigations
GPS	Board-owned vehicles	GPS tracking system	H&S of employees and public, Security of board assets, Service improvement. Administrative investigations.

SMCDSB Supported/Managed Applications	Uses of those applications	Embedded tools in supported/managed applications	Protect against unauthorized access and monitor overall usage. Troubleshooting and support.
System Logging	Information Systems	System logs	To comply with privacy laws. Troubleshooting and support.
Printing	Printed Document	Printer Management Software	Billing/Useage. Troubleshooting and support.

Approved: Board Meeting #16-2013 (Wednesday, November 27, 2013)
Revised: Board Meeting #6-2018 (Wednesday, April 25, 2018)
Revised: Board Policy Review Meeting #04-2022 (Wednesday May 11, 2022)
Revised: Board Meeting #08 (Wednesday, June 15, 2022)
Reviewed: Board Policy Review Meeting (Wednesday, December 14, 2022)
Reviewed: Board Meeting #03-2023 (Wednesday, January 18, 2023)