

---

## **Administrative Procedures Memorandum A1300 – Information and Computing Technology – Appropriate Use Guidelines for Students**

<b>Date of issue</b>	August 2025
<b>Contact</b>	Information Technology Services School Services
<b>References</b>	<a href="#">Policy 4181 – Plagiarism and Cheating</a> <a href="#">APM A1460 – Assessment, Evaluation, and Reporting</a> <a href="#">APM A7630 – Code of Conduct</a> <a href="#">APM A7635 – Student Discipline Procedures</a> <a href="#">International Society for Technology in Education</a> <a href="#">Copyright Act of Canada</a> <a href="#">Criminal Code of Canada</a>

---

### **1. Background**

The Simcoe County District School Board (SCDSB) provides students with a digital media learning environment comprised of information and computing technologies (ICT) which may include software, internet access, and hardware (e.g., computers, tablets, Chromebooks, printers, scanners, digital cameras, etc.). This procedure sets out standards for appropriate student use of ICT, including board and personally-owned equipment for educational purposes while at school or at school-sponsored activities. Annual acknowledgement and agreement by parents/guardians and students to the Student ICT Appropriate Use Agreement ([Form A1300 – 1](#)) is required.

### **2. Definitions**

- 2.1 Board-provisioned technology – includes hardware, networks, and software provided by the Simcoe County District School Board (SCDSB) for job-related and educational purposes.
- 2.2 Digital citizenship – the International Society for Technology in Education (ISTE) defines it as the norms of appropriate, responsible technology use.
- 2.3 Digital footprint – the information about an individual that exists on the internet as a result of their online activity.
- 2.4 Harassment – engaging in a course of vexatious comment or conduct that is known or ought reasonably to be known to be unwelcome.
- 2.5 ICT – includes use of networks, information systems and applications, and any device that connects to the network, whether used within the board or in a way that has a connection to the board.

- 
- 2.6 Internet – the computer network systems connecting electronic devices all over the world through which individual subscribers can interact and share information.
  - 2.7 Plagiarism – taking the writings or ideas of others and presenting them as if they were original.
  - 2.8 Social media – a form of online publication or presence that allows end users to engage in multi-directional conversations in or around the content of a website. Social media includes, but is not restricted to, social networking, blogs, wikis, podcasts, forums, content communities, emails, instant messaging, and texting.
  - 2.9 Third-party application – any software or online tool that has not been developed by the SCDSB.

### **3. Use**

- 3.1 ICT is available for student use to support appropriate instructional practices aligned with curriculum expectations.
- 3.2 Student use of ICT will be in accordance with the laws of Canada and Ontario (e.g., *Copyright Act*, *Criminal Code of Canada*, and the *Education Act*), and Board policies and procedures (e.g., Administrative Procedures Memorandum [APM] A7635 - Student Discipline Procedures and APM A7630 – Code of Conduct).
- 3.3 Safe use of ICT is supported by appropriate instruction on safe use, technological tools such as internet filtering and blocking, standards of behaviour, and consequences for inappropriate behaviour.
- 3.4 Students will treat board ICT with respect and care, including reporting known technical, safety, or security problems.
- 3.5 The onus is on the student to use ICT appropriately.
- 3.6 Students are responsible for connecting personal devices to the network and for altering settings as necessary on their own devices to connect. Board staff will not connect student devices for them.
- 3.7 Personal devices are only to be connected to the guest wireless network and not be plugged into any SCDSB networks using an ethernet cable. Devices should be easily identifiable, clearly labeled, and where possible, registered with the manufacturer.

---

#### **4. Digital citizenship**

- 4.1 Digital media learning environments use ICT to help students communicate and work collaboratively, support individual learning, and contribute to the learning of others while gaining skills required to be productive and safe digital citizens. Applications are used as instructional tools. They allow students to:
  - 4.1.1 interact and publish with peers, experts, and others;
  - 4.1.2 communicate information and ideas effectively to multiple audiences;
  - 4.1.3 develop cultural understanding and global awareness by engaging with learners of other cultures; and,
  - 4.1.4 contribute to project teams to produce original works or solve problems.
- 4.2 Staff will review the appropriate use agreement ([Form A1300 – 1](#)) with students at the start of the school year or semester.
- 4.3 Students will receive appropriate instruction on digital citizenship and responsible use of technology in alignment with the Ontario curriculum.
- 4.4 When using communications and online tools, students are reminded that appropriate behaviour and anti-bullying guidelines apply in the online world. Protecting their privacy, safety, and reputation and the privacy, safety, and reputation of others is essential.

#### **5. Inappropriate use/activities**

- 5.1 Students will not:
  - 5.1.1 attempt to gain unauthorized access, such as hacking into the SCDSB network or any other computer system using ICT. This includes plugging network cables into personal devices. All personal devices must connect to the guest wireless network only;
  - 5.1.2 share passwords, except as may be required by Information Technology Services staff for maintenance and support purposes;
  - 5.1.3 log into anyone else's account, nor will they attempt to access the personal data of others;
  - 5.1.4 deliberately attempt to disrupt the computer system performance or to destroy data by spreading computer viruses or by using other means. These actions may be illegal. Any attempt to do so will be referred to the appropriate authorities;
  - 5.1.5 use ICT to engage in any illegal activities;
  - 5.1.6 use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language;
  - 5.1.7 engage in any behaviour that may contribute to a negative school climate (e.g., racial slurs, jokes, teasing);
  - 5.1.8 share information that, if acted upon, could cause damage or danger of disruption to the system or bring about harm to others;
  - 5.1.9 harass others;
  - 5.1.10 cyberbully others;

- 
- 5.1.11 knowingly or recklessly post false or defamatory information about a person or organization;
  - 5.1.12 share private/personal information about another person;
  - 5.1.13 access, store, or distribute material that encourages conduct that would be a criminal offence or give rise to civil liability. This includes materials that are profane or obscene (e.g., pornography), that advocate illegal or dangerous acts, or that advocate violence or discrimination towards other people (e.g., hate literature). A special exception may be made if the purpose is to conduct research, and both the staff member and the parent/guardian approve access. If a student inadvertently accesses such information, they must immediately disclose the inadvertent access to the supervising staff member; and,
  - 5.1.14 use ICT to record (audio or video) or photograph other students or staff unless authorized by SCDSB staff prior to any recordings being made. This is to respect the privacy and ensure the safety of all students and staff.

## **6. Security and safeguards**

- 6.1 The SCDSB uses appropriate internet filtering and blocking to reduce the risk of staff accessing inappropriate content online. No software can block all inappropriate material. Filtering is used on board-provisioned computers and BYOD connected to the board's guest wireless network.
- 6.2 Students are responsible for the use of their individual account and will take all reasonable precautions to prevent others from being able to access and use their account.
- 6.3 Students will exercise care when setting and managing passwords to protect themselves and their personal information. This includes creating complex passwords that cannot be easily guessed. The use of a passphrase instead of a single-word password is recommended, as they are easy to remember but hard to guess. All passwords will be a minimum of 14 characters in length.
- 6.4 Students must not share their password, except with staff when necessary to obtain technical support and assistance. If a password has been shared with staff, it must be changed immediately following service.
- 6.5 Students will immediately notify the administrator if they have identified a possible security problem. Students will not intentionally search out security problems. This may be construed as an illegal attempt to gain access.

---

**7. Expectation of privacy**

- 7.1 Online work is not private. Staff may access student digital media workspaces for assessment and support purposes, to maintain system integrity, and to ensure that students are using the system responsibly and safely. A search may be conducted if there is reasonable cause to suspect that a student has violated the law, APM A7630 – Code of Conduct, or the Student ICT Appropriate Use Agreement ([Form A1300 – 1](#)).
- 7.2 When working online, students will practice safe computing practices, including:
- 7.2.1 protecting their identity;
  - 7.2.2 not posting personal information about themselves and others (the internet is a public place); and,
  - 7.2.3 protecting their digital footprint (what goes online stays online).

**8. Plagiarism and copyright infringement**

- 8.1 Students will not plagiarize works they find on the Internet. Plagiarism is taking the writings or ideas of others and presenting them as if they were original to the student. SCDSB [Policy 4181 – Plagiarism and Cheating](#) and [APM A1460 – Assessment, Evaluation, and Reporting](#) contain information and guidelines related to plagiarism.
- 8.2 Students will respect the rights of copyright owners and will not download protected works (e.g., images, movies, music, etc.). Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by copyright. If a work contains language that specifies appropriate use of that work, the student should follow the expressed requirements. If the student is unsure whether they can use a work, they should request permission from the copyright owner.
- 8.3 SCDSB software is for school use unless licensed otherwise. Use of SCDSB licensed software on equipment for which it is not licensed is a copyright infringement and is **illegal**.
- 8.4 Use of software on SCDSB equipment that is not licensed for use on SCDSB equipment is a copyright infringement and is **illegal**.

**9. Responsibilities of parents/guardians**

- 9.1 Parents/guardians and adult students must review, agree to, and sign the Student ICT Appropriate Use Agreement ([Form A1300 – 1](#)) at the start of each school year.
- 9.2 Parents/guardians may request the termination of their child(ren)'s individual account.

---

**10. Response guidelines**

- 10.1 The SCDSB will cooperate fully with local, provincial, or federal officials in any investigation concerning or relating to any illegal activities conducted at school, during school-sponsored activities, or that impact the school.
- 10.2 Routine maintenance, monitoring, and surveillance of the system may lead to the discovery that a student has been or is in violation of the Student ICT Appropriate Use Agreement ([Form A1300 – 1](#)), and/or the law.
- 10.3 In the event of an allegation of a violation of the Student ICT Appropriate Use Guidelines ([Form A1300 – 1](#)), the student will be provided with a notice and an opportunity to be heard in the manner set forth in APM A7630 – Code of Conduct and/or SCDSB policies and procedures.
- 10.4 A search of student files, records of activities, and related information will be conducted if there is reasonable suspicion that a student has violated APM A7630 – Code of Conduct, the Student ICT Appropriate Use Agreement ([Form A1300 – 1](#)), or the law. The nature of the investigation will be reasonable and in keeping with the context of the alleged violation.
- 10.5 Any violation of APM A7630 – Code of Conduct, the Student ICT Appropriate Use Agreement ([Form A1300 – 1](#)), or the law may result in confiscation of personally owned equipment and appropriate discipline. Confiscated equipment may be returned to the parents/guardians or, in the event of suspected illegal or inappropriate activity, may be forwarded to the appropriate law enforcement agency.
- 10.6 Disciplinary actions will be in accordance with [APM A7635 – Student Discipline Procedures](#).
- 10.7 Computer privileges of a student may be suspended by the administrator or designate.

***Issued under the authority of the Director of Education***

**First issued:** June 2012

**Revised:** August 2013, October 2013, May 2017, June 2022, August 2025