Date of Issue	May 2017
Original Date of Issue	June 2012
Subject	**INFORMATION AND COMPUTING TECHNOLOGY - APPROPRIATE USE GUIDELINES FOR STUDENTS**
References	This APM replaces A1160 – Computing and Information Technology – Acceptable Use Policy 4181- Plagiarism and Cheating APM A1460 - Assessment, Evaluation and Reporting
Contact	Information Technology Services; School Services

1. Purpose

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, hardware (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 on school-sponsored activities. Parents'/guardians'/students' acknowledgement and agreement of the Student Information Computing Technology (ICT) Appropriate Use Agreement is required annually (see FORM A1300 - 1).

2. Use

2.1 ICT is available for student use to support appropriate instructional practices aligned with curriculum expectations.

2.2 Student use of ICT shall be in accordance with the laws of Canada and Ontario (e.g. Copyright Act, Criminal Code of Canada, and the Education Act), Board Policies and Procedures (e.g. Student Discipline Procedures and the School and Board Code of Conduct).

2.3 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.

2.4 Students shall treat board ICT with respect and care, including reporting known technical safety or security problems.

2.5 The onus is on the student to use ICT appropriately.

2.6 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. Digital Citizenship

3.1 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. Students use a variety of applications that may include blogs, wikis, learning management systems (such as Google Classroom, Google Drive, Moodle, Desire 2 Learn (D2L) Edmodo) and social networking sites (such as Facebook, Twitter, YouTube, etc.). When these applications are used as instructional tools, they allow students to:

- 3.1.1 interact and publish with peers, experts and others;
- 3.1.2 communicate information and ideas effectively to multiple audiences;
- 3.1.3 develop cultural understanding and global awareness by engaging with learners of other cultures; and,
- 3.1.4 contribute to project teams to produce original works or solve problems.

3.2 Teachers shall review the appropriate use agreement with students at the start of school year/semester and a copy shall be posted in the classroom for reference.

3.3 **Respect, Educate and Protect (REP)**

Students receive appropriate instruction on digital citizenship based on nine elements of using technology appropriately developed by the International Society for Technology in Education (ISTE). Each area encompasses three elements of digital citizenship. Please refer to the ISTE website for more information.

3.3.1 **Respect Your Self/Respect Others**

- 3.3.1.1 Etiquette
- 3.3.1.2 Access
- 3.3.1.3 Law

3.3.2 **Educate Your Self/Connect with Others**

- 3.3.2.1 Communication
- 3.3.2.2 Literacy
- 3.3.2.3 Commerce

3.3.3 **Protect Your Self/Protect Others**

- 3.3.3.1 Rights and Responsibility
- 3.3.3.2 Safety (Security)
- 3.3.3.3 Health and Welfare

4. Inappropriate Use/Activities

4.1 Students shall not:

- 4.1.1 attempt to gain unauthorized access, such as hacking into the SCDSB network or to 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;
- 4.1.2 share passwords, except as may be required by Information Technology Services staff for maintenance and support purposes;

4.1.3 log into anyone else's account, nor will they attempt to access the personal data of others;

4.1.4 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, shall be referred to the appropriate authorities;

4.1.5 use ICT to engage in any illegal activities;

4.1.6 use obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language;

4.1.7 use racial slurs, comments, jokes or teasing and defamatory or discriminatory communications and postings, graffiti and other behaviour that might cause a negative school climate;

4.1.8 share information that, if acted upon, could cause damage or danger of disruption to the system or bring about harm to others;

4.1.9 harass others; (harassment is persistently acting in a manner that distresses or annoys another person);

4.1.10 cyberbully others;

4.1.11 knowingly or recklessly post false or defamatory information about a person or organization;

4.1.12 share private information about another person;

4.1.13 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 (pornography), that advocate illegal or dangerous acts, or that advocate violence or discrimination towards other people (hate literature). A special exception may be made if the purpose is to conduct research and both the teacher and the parent approve access. If a student inadvertently accesses such information, they must immediately disclose the inadvertent access to the supervising teacher; and,

4.1.14 use ICT to record or photograph other students or staff unless authorized by school teaching or administrative staff prior to any recordings being made. Such equipment includes board and personally-owned devices, such as cell phones, smart phones, iPods, iPads, computers, personal digital assistants (PDAs), cameras, MP3 players, tape recorders, video-recorders, digital audio recorders and any other technological equipment that allows for recordings to be made of visual images and/or sounds. This is to respect the privacy and ensure the safety of all students and staff.

5. Security/Safeguards

5.1 The SCDSB uses appropriate Internet filtering and blocking to reduce the risk of students accessing inappropriate content online; however, no software is capable of blocking all inappropriate material. Filtering is used on board-owned computers and personally-owned devices connected to the board network.

5.2 Students are responsible for the use of their individual account and shall take all reasonable precautions to prevent others from being able to access and use their account.

5.3 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.

5.4 Students will immediately notify the system 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.

5.5 Students will avoid the inadvertent spread of computer viruses by using virus protection procedures when downloading software.

5.6 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. Password complexity should include a unique combination of words, numbers, symbols and/or both upper and lower case characters. All passwords will be a minimum of eight characters and should be changed on a regular basis.

6. Expectation of Privacy

6.1 **Students should not expect that online work is private.** Staff may access student digital media work spaces 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, the Code of Conduct or the Student Information Computing Technology Appropriate Use Agreement.

6.2 When using social networking sites outside of the classroom (i.e. in their homes), students are reminded that appropriate behaviour and anti-bullying guidelines apply in the online world. Protect your privacy, safety and reputation and the privacy, safety and reputation of others.

6.3 **When working online, students shall practice safe computing practices including:**

6.3.1 protecting their identity and reputation;

6.3.2 not posting personal information about themselves and others (the Internet is a public place); and,

6.3.3 protecting their digital footprint (what goes online stays online).

7. Plagiarism and Copyright Infringement

7.1 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. (See Policy 4181 Plagiarism and Cheating and APM1460 Assessment, Evaluation and Reporting.)

7.2 Students will respect the rights of copyright owners and shall not download protected works (i.e. images, movies and 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 or not they can use a work, they should request permission from the copyright owner.

7.3 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**.

7.4 Use of software on SCDSB equipment that is not licensed for use on SCDSB equipment is a copyright infringement and **illega**l.

8. Responsibilities of Parents

8.1 Parents/guardians must review, agree to, and sign the Student ICT Appropriate Use Agreement at the start of each school year.

8.2 Parents/guardians may request the termination of their child(ren)'s individual account.

8.3 The SCDSB Appropriate Use Guidelines for Students contain restrictions on accessing inappropriate materials. Student use will be supervised during instructional time. Parents/guardians should be advised that a wide range of materials are available from the Internet, some of which may not be fitting with the particular values of their families. Parents/guardians are encouraged to specify to their child(ren) those materials which are not appropriate for their child(ren) to access.

9. Due Process

9.1 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.

9.2 In the event of an allegation of a SCDSB Appropriate Use Guidelines for Students violation, the student will be provided with a notice and an opportunity to be heard in the manner set forth in the Code of Conduct and/or SCDSB policies and procedures.

9.3 Disciplinary actions shall be in accordance with APM 7635 - Student Discipline Procedures.

9.4 Computer privileges of a student may be suspended by the principal.

10. Search and Seizure

10.1 A search may be conducted if there is reasonable cause to suspect that a student has violated the law, the Code of Conduct or the Student Information Computing Technology (ICT) Appropriate Use Agreement.

10.2 Routine maintenance, monitoring and surveillance of the system may lead to discovery that a student has been or is in violation of the SCDSB Appropriate Use Guidelines for Students and/or the law.

10.3 A search of student files, records of activities, and related information will be conducted if there is reasonable suspicion that a student has violated the SCDSB Appropriate Use Guidelines for Students or the law. The nature of the investigation will be reasonable and in keeping with the context of the alleged violation.

10.4 Any violation of the Student Information Computing Technology Appropriate Use Agreement may result in confiscation of personally-owned equipment and appropriate discipline. Confiscated equipment may be returned to the parent/legal guardian or, in the event of suspected illegal or inappropriate activity, may be forwarded to the appropriate law enforcement agency.

STUDENT INFORMATION COMPUTING TECHNOLOGY (ICT) APPROPRIATE USE AGREEMENT

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, hardware (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 on school-sponsored activities. Parents'/guardians'/students' acknowledgement and agreement of the Student ICT Appropriate Use Agreement is required annually.

Digital media learning environments use ICT to help students communicate and work collaboratively, and contribute to the learning of others while gaining skills required to be productive and safe digital citizens. Students use a variety of applications which may include blogs, wikis, learning management systems (such as Google Classroom, Google Drive, Moodle, Desire 2 Learn (D2L), Edmodo) and social networking sites (such as Facebook, Twitter, YouTube, etc.). When these applications are used as instructional tools, they allow students to:

- interact and publish with peers, experts and others;
- communicate information and ideas effectively to multiple audiences;
- develop cultural understanding and global awareness by engaging with learners of other cultures; and,
- contribute to project teams to produce original works or solve problems.

The following safeguards are used to reduce the risk of accessing or viewing inappropriate content online and for student safety.

1. **Digital Citizenship -** Students receive appropriate instruction on digital citizenship and safe computing practices based on nine elements of using technology appropriately developed by the International Society for Technology in Education (ISTE). Teachers will review the Student ICT Appropriate Use Agreement with students at the start of each school year/semester and a copy shall be posted in the classroom for reference.

2. **Internet Filtering and Blocking -** The SCDSB uses appropriate Internet filtering to reduce the risk of students accessing inappropriate content online. However, no software is capable of blocking all inappropriate material. Filtering is used on board-owned computers and personally-owned devices connected to the board network.

3. **Classroom Supervision –** School staff monitor by observation and through online programs to support focussed, purposeful use of ICT when a student is online during the school day.

4. **Code of Conduct/Discipline Procedures -** The school Code of Conduct (see student agenda) sets out rules for student behaviour including online activity. Inappropriate use is subject to discipline in accordance with the school discipline policy and procedure. Students who are experiencing and/or witness any form of harassing, defaming and/or bullying shall report to a school official.

Appropriate Use

- ICT is available for student use to support appropriate instructional practices aligned with curriculum expectations.
- Use of ICT shall be in accordance with the laws of Canada and Ontario (e.g. Copyright Act, Criminal Code of Canada, and the Education Act), Board Policies and Procedures (e.g. Student Discipline Procedures) and the School and Board Code of Conduct.
- ICT use shall be in accordance with safe computing practices.
- Students will treat board ICT with respect and care, including reporting known technical, safety or security problems.
- Students are responsible for the use of their individual account and shall take all reasonable precautions to prevent others from being able to access and use their account. The onus is on the student to use ICT appropriately.
- When using social networking sites outside of the classroom (i.e. in their homes), students are reminded that appropriate behaviour and anti-bullying guidelines apply in the online world. Protect your privacy, safety and reputation and the privacy, safety and reputation of others.
- 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. Password complexity should

include a unique combination of words, numbers, symbols and/or both upper and lower case characters. All passwords will be a minimum of eight characters and should be changed on a regular basis.

Inappropriate Use/Activities

Students **shall not**:

- attempt to gain unauthorized access (e.g. hacking) into any computer system;
- share passwords, except as may be required by staff for maintenance and support purposes;
- login to anyone else's account, or access the personal data of others;
- deliberately attempt to disrupt the computer system performance or to destroy data by spreading computer viruses or by using other means;
- share information that, if acted upon, could cause damage or danger of disruption to the system or bring about harm to others;
- engage in cyberbullying;
- share private information about another person;
- access, store or distribute material that is profane or obscene (including pornography), that advocate illegal or dangerous acts, or that advocate violence or discrimination towards other people (hate literature); and,
- use ICT to record or photograph other students or staff unless authorized by school teaching or administrative staff prior to any recordings being made. Such equipment includes board and personally-owned devices, such as cell phones, smart phones, iPods, iPads, computers, personal digital assistants (PDAs), cameras, MP3 players, tape recorders, video-recorders, digital audio recorders and any other technological equipment that allows for recordings to be made of visual images and/or sounds. This is to respect the privacy and ensure the safety of all students and staff.

Students should not expect that online work is private. Staff may access student digital media work spaces 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, the Code of Conduct or this agreement.

The decision to allow a student to bring a personally-owned device to school rests with the parent and the student. The board and the student's school will not be responsible for devices that are lost, stolen or damaged in any manner. Students are responsible for connecting their own devices to the guest wireless network. Help documents are available, but board staff will not be responsible for connecting student devices. 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. Any violation of this agreement may result in confiscation of personally-owned equipment and appropriate discipline. Confiscated equipment may be returned to the parent/guardian or, in the event of suspected illegal or inappropriate activity, may be forwarded to the appropriate law enforcement agency.

Parents/guardians must recognize that a wide range of materials are available from the Internet, some of which may not be fitting with the particular values of their families.

- I have read the Student ICT Appropriate Use Agreement and understand that I must follow the terms of use outlined in the agreement relating to computer use.

- In the event that my child chooses to bring a personally owned device, I understand that the SCDSB and the school accepts no responsibility for the loss, theft, or damage of my/my child's device and that it will be my/my child's responsibility to appropriately manage the device at school, including access to the guest wireless network.

Parent/Guardian/Adult Student Name	Parent/Guardian/Adult Student Signature
Student Name	Student Signature
Date	School Name