Date of Issue	May 2017
Original Date of Issue	August 2013
Subject	**INFORMATION AND COMPUTING TECHNOLOGY AND INTERNET APPROPRIATE USE GUIDELINES FOR EMPLOYEES**
References	This APM replaces APM A1160 - Computing and Information Technology - Acceptable Use Policy 4181 - Cheating and Plagiarism APM A1450 - Management of Personal Information - Student APM A1452 - Privacy Breach Protocol APM A1460 - Assessment, Evaluation and Reporting APM A1063 - Use of Copyright-Protected Works for Education Provincial Code of Conduct (PPM 128) OCT Advisory - Use of Electronic Communication and Social Media International Society for Technology in Education (ISTE) NETS for Teachers
Contact	Information Technology Services; Human Resources

1. Purpose

1.1 This procedure sets out standards for appropriate employee use of Information and Computer Technology (ICT) for educational and job related purposes. All employees are subject to this procedure.

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 **Bring Your Own Device (BYOD)** - ICT that is not provided by the SCDSB.

2.3 **Digital Citizenship** – The International Society for Technology in Education (ISTE) defines it as the norms of appropriate, responsible technology use. Refer to the Digital Citizenship Page on the staff website for more information.

2.4 **Information and Computing Technology (ICT)** includes use of networks and equipment that connects to the network (i.e. computers, tablets, smartphones), as well as the use of information systems and applications such as computer software, electronic mail, web pages and the internet whether used within the board or in a way that has a connection to the board. The definition of ICT also includes BYOD when used on board networks or board/job related purposes.

2.5 **Internet** - the computer network systems connecting electronic devices all over the world through which individual subscribers can interact and share information.

2.6 **Social media** – is 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.

3. Responsibilities

3.1 **Board**
The Board will provide employees with board-provisioned technology to perform their assigned duties.

3.2 **Supervisor**
Superintendents/principals/managers shall review the appropriate use agreement with new employees and annually with all employees. This agreement is available for reference on the SCDSB Staff website.

3.3 **Employees**
Employees shall:

3.3.1 Be aware of, and comply with, the rules of appropriate use of ICT as set out in this procedure.

3.3.2 Protect their passwords and system access by taking all reasonable precautions to prevent others from being able to access and use their account and/or assume their identity. Passwords may only be shared with ITS staff for technical support and assistance and must be changed immediately following service.

3.3.3 Use board-approved data storage medium and security measures (i.e. encryption) for the handling and storage of board records and information assets.

3.3.4 Shall treat board ICT with respect and care including reporting known technical safety or security problems. Responsibility to protect the physical safety and privacy of information on all assigned ICT (i.e. computers, cellular phones, teaching notebooks) is the responsibility of the employee.

3.3.5 Ensure that their online activity does not interfere with their work commitment.

4. Appropriate Use

The onus is on the employee to use ICT appropriately as outlined in this procedure.

4.1 Use of SCDSB ICT shall be in compliance with:

4.1.1 Standards of courtesy and behaviour consistent with the Provincial Code of Conduct (PPM 128) and SCDSB APM A7630, Code of Conduct. These norms apply to all individuals involved in the publicly-funded school system whether they are on school property, at school-related events or activities, or in other circumstances that could have an impact on the school climate.

4.1.2 The laws of Canada and Ontario including:

4.1.2.1 The *Education Act* (statutory duty of confidentiality);

4.1.2.2 The *Municipal Freedom of Information and Protection of Privacy Act;*

4.1.2.3 The *Canadian Copyright Act* and the SCDSB APM A1063, Use of Copyright-Protected Works for Education; and,

4.1.2.4 The *Criminal Code* of Canada.

4.1.3 Board Policies and Procedures.

4.1.4 For members of the Ontario College of Teachers - the ethical standards for the teaching profession and the Professional Advisory - Use of Electronic Communication and Social Media. Refer to the OCT website (www.oct.ca/en) for more detailed information.

4.1.5 Software licensing agreements and terms of use statements.

5. Inappropriate Use/Activities

Employees shall not:

5.1 Attempt to gain unauthorized access such as, hacking into the SCDSB network or into any other computer system. This includes plugging network cables into personal devices. All personal devices must connect to the wireless guest network only.

5.2 Share passwords, except as may be required by Information Technology Services (ITS) staff for maintenance and support purposes.

5.3 Login to another person's account, or attempt to access the personal data of others.

5.4 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.

5.5 Use obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language.

5.6 Use racial slurs, comments, jokes or teasing and defamatory or discriminatory communications and postings, graffiti and other behaviour that might cause a negative climate or work environment.

5.7 Share information that, if acted upon, could cause damage or danger of disruption to the system or bring about harm to others.

5.8 Harass others; harassment is defined as engaging in a course of vexatious comment or conduct that is known or ought reasonably to be known to be unwelcome.

5.9 Knowingly or recklessly post false or defamatory information about a person or organization.

5.10 Share private information about another person, including their likeness or image without their consent.

5.11 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 the

superintendent/principal/manager approves access. If an employee inadvertently accesses such information, they are to immediately disclose the inadvertent access to the superintendent/ principal/ manager.

5.12 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 employee.

5.13 Use board-provisioned technology for personal gain/profit.

6. Social Media

6.1 The evolution of the internet and social media sites has fundamentally changed how we communicate and collaborate with teachers, students, parents and communities. While collaboration in the online world can be a very powerful teaching tool, employees must remember that:
- 6.1.1 the internet and social media sites are public places;
- 6.1.2 what goes online stays online and may never be fully erased; and,
- 6.1.3 in the online world people may not always be who they say they are.

6.2 Digital Citizenship sets out norms for using social media.

6.3 When using social media employees shall practice safe computing practices including:
- 6.3.1 protecting their identity and reputation;
- 6.3.2 not posting personal information about self and others (the internet is a public place); and,
- 6.3.3 protecting their digital footprint (what goes online stays online).

6.4 Personal information about an identifiable or potentially identifiable individual shall not be posted on the internet without the written consent of person or the parent/guardian (refer to APM A1450, Management of Personal Information - Student for consent forms). This includes information that students will be self-posting as part of a class assignment. Note personal information is defined by the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA). For a comprehensive definition refer to APM A1450, Management of Personal Information - Student.

6.5 When seeking consent for posting online, the parent/guardian shall be provided with an overview of the activity which clearly states expectations and guidelines for students. Should a parent/adult student choose not to participate, the teacher shall find a suitable educational alternative for the student.

6.6 Employee shall block or suppress (Blind carbon copy – Bcc) the display of email address where this capability exists.

7. Personal Use of Social Media

7.1 Employees should use these sites with the same professionalism and responsibility as they would when officially representing the board, presenting themselves with the highest of standards.

7.2 Employees should not engage in board business or discussions regarding the board from a personal perspective.

7.3 When using social media outside of their place of employment (i.e. in their homes), employees are reminded that the Provincial Code of Conduct applies. Protect your privacy, safety and reputation and the privacy, safety and reputation of others.

7.4 Employees shall not use personal social media sites to communicate with students. It is inappropriate to have students as “friends” on these sites and any invitations from students to join a social network site should be declined.

7.5 In using social media sites, employees should be encouraged to make sure their privacy settings for both content and photos are set. Employees should carefully screen who can post on their site.

7.6 All inappropriate references to the board, to schools or school personnel, students, parents/guardians or any other member of the school community, in computer-related mediums, such as social networking sites, blogging, web pages or e-mail, represents a contravention of Board policy.

7.7 Employees who have a personal social media site in which they indicate their position or place of work, should discuss any potential conflicts of interest with their superintendent/principal/manager or appropriate school administrator. Similarly, employees who want to start blogging - and wish to say that they work at the school - should discuss any potential conflicts of interest with the principal or appropriate supervisor.

7.8 Employees shall ensure that social media sites do not reveal personal or confidential information about its employers, students, parents/guardians or other members of the school community. This may include photographs or videos of students or employees, curricular information, financial information, school plans, and school development information.

7.9 Confidential school information should not be placed on a social media site without the express consent of the superintendent/principal/manager.

7.10 Employees shall ensure that their online activity does not interfere with their work commitment.

8. Security/Safeguards

8.1 The SCDSB uses appropriate internet filtering and blocking to reduce the risk of employees accessing inappropriate content online. No software is capable of blocking

all inappropriate material. Filtering is used on board-provisioned computers and BYOD connected to the board's guest wireless network.

8.2 Employees will exercise care when setting and managing passwords to protect themselves, our students and the Board. 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.

8.3 Employees shall immediately notify ITS staff and/or supervisor if they have identified a possible security problem. Employees will not intentionally search out security problems. This may be construed as an illegal attempt to gain access.

8.4 Breaches of personal information shall be managed in accordance with APM A1452, Privacy Breach Protocol.

9. Employer Access/Expectation of Privacy

9.1 Employees should not expect that their use of ICT is private.

9.2 Employer access to ICT shall be for the following purposes to:
- 9.2.1 engage in technical maintenance, repair and management;
- 9.2.2 meet a legal requirement to produce records including engaging in e-discovery;
- 9.2.3 ensure continuity of work processes (i.e. employee departs, employee gets sick, work stoppage occurs, etc.); and,
- 9.2.4 prevent misconduct and ensure compliance with the law.

9.3 A search may be conducted if there is reasonable cause to suspect that an employee has violated the law, the Provincial Code of Conduct or the Information and Computing Technology - Appropriate Use Guidelines for Employees.

9.4 A search of employee files, records of activities, and related information will be conducted if there is reasonable suspicion that an employee has violated the Information and Computing Technology - Appropriate Use Guidelines for Employees and/or the law. The nature of the investigation will be reasonable and in keeping with the context of the alleged violation.

9.5 The SCDSB will cooperate fully with local, provincial, or federal officials in any investigation concerning or relating to any illegal activities conducted in the workplace, during school sponsored activities or that impact the school.

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

9.7 Discipline shall be in accordance with the Guide to the Principles of Progressive Discipline.

10. Bring Your Own Devices (BYOD)

10.1 ITS staff will not provide hands-on support of personally owned devices, which includes connecting them to the guest wireless network. The support is limited to documentation that may be provided to assist with connection of certain devices to the network. The Board assumes no responsibility to ensure that all devices are able to connect to the network. In the event that an employee chooses to bring a BYOD, it is understood that the SCDSB and the school accepts no responsibility for the loss, theft, or damage of the employee's device and that it will be the responsibility of the employee to appropriately manage the device at work.

10.2 To ensure board access and protection of privacy, board records shall not be stored on BYOD.

10.3 Employees who choose to use a BYOD device do so on the understanding that they may be sacrificing personal privacy.

10.4 Any violation of this procedure may result in confiscation of personally-owned equipment and appropriate discipline. Confiscated equipment may be returned to the employee or in the event of suspected illegal or inappropriate activity it may be forwarded to the appropriate law enforcement agency.

First Issued August 2013
Revised May 2017

Issued under the authority of the Director of Education