Date of Issue	August 2023
Original Date of Issue	August 2013
Subject	**INFORMATION AND COMPUTING TECHNOLOGY AND INTERNET APPROPRIATE USE GUIDELINES FOR EMPLOYEES**
References	Policy 4181 – Cheating and Plagiarism APM A1063 – Use of Copyright-protected Works for Education APM A1450 – Management of Personal Information Student APM A1452 – Privacy Breach Protocol APM A1460 – Assessment, Evaluation and Reporting International Society for Technology in Education (ISTE) NETS for Teachers OCT Advisory – Use of Electronic Communication and Social Media PPM 128 – Provincial Code of Conduct
Contact	Information Technology Services; Human Resource Services

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 StaffWeb for more information.

2.4 Digital footprint – the information about an individual that exists on the internet as a result of their online activity.

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. The definition of ICT also includes BYOD when used on board networks, information systems, and applications ~~or~~ for board/job-related purposes.

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 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.

2.8 Third party application – any software or online tool that has not been developed by the SCDSB.

3. Responsibilities

3.1 SCDSB
The board shall provide employees with board-provisioned technology to perform their assigned duties.

3.2 Supervisors (superintendents/principals/managers)
Supervisors shall:
3.2.1 ensure new employees review and agree to the appropriate use guidelines outlined in this procedure;
3.2.2 review the appropriate use guidelines annually with all employees; and,
3.2.3 ensure that the responsibilities of employees with regards to board-owned technology are acknowledged on an annual basis, through mandatory training declarations.

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. When required by Information Technology Services (ITS) staff for technical support and assistance, passwords may be changed by ITS 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 treat board ICT with respect and care including reporting known technical safety or security problems. Protection of the physical safety and privacy of information on all assigned ICT (e.g., computers, cellular phones, teaching notebooks) is the responsibility of the employee. The employee will reimburse the SCDSB for the full replacement or repair cost, as determined by ITS, of any technology that is damaged, lost or stolen due to the employee’s lack of respect or care. The employee will receive an invoice from ITS which will provide direction with regards to reimbursement to the SCDSB;
3.3.5 ensure their online activity does not interfere with their work commitments; and,
3.3.6 participate in board provided Cyber Security Awareness training that is delivered to new hires, during professional development~~s~~ days, and cyber security awareness campaigns throughout the year.

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 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 (MFIPPA);*

4.1.2.3 the *Canadian Copyright Act* and 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 (OCT) - the ethical standards for the teaching profession and the Professional Advisory - Use of Electronic Communication and Social Media. Refer to the OCT website 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 or plugging network cables into personal devices. All BYOD must connect to the wireless guest network only.

5.2 Share passwords with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, confidential board information.

5.3 Login to another person’s account, or attempt to access the personal data of others, except as required by ITS staff for maintenance, support or when required by execution of assigned duties.

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, disrespectful, or harmful 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 (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 the supervisor approves access. If an employee inadvertently accesses such information, they are to immediately disclose the inadvertent access to the supervisor.

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 their 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/guardians 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; and,
6.3.3 protecting their digital footprint.

6.4 Personal information about an identifiable or potentially identifiable individual shall not be posted on the internet without the written consent from that person or the student's parent/guardian. This includes information that students will be self-posting as part of a class assignment. Personal information is defined by MFIPPA.- For consent forms and 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/guardian or adult student choose not to participate, the teacher shall find a suitable educational alternative for the student.

6.6 Employees shall block or suppress (blind carbon copy – Bcc) the display of email addresses 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 (e.g., in their homes), employees are reminded that the Provincial Code of Conduct applies. Protect your privacy, safety, and reputation as well as 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. Any invitations from students to join a social network site should be declined.

7.5 When 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 email, represent 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 supervisor 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 their employers, students, parents/guardians, or other members of the school community. This may include photographs and/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, or manager.

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

8. Third Party Applications

8.1 There are many types of applications and online tools, and their terms and conditions and privacy policies can vary. Ontario school boards must comply with MFIPPA. MFIPPA protects personal information by limiting when and how it can be collected, used, and disclosed. Before classroom use, staff are expected to confirm that the application has been reviewed by the Educational Computing Network of Ontario (ECNO) for privacy and security and by the SCDSB for use by reviewing the Use of Third-Party Applications for Educators page on the StaffWeb. Staff must review the approval status that SCDSB has assigned to the application and follow instructions provided in the Resource Document which is also located on the Use of Third-Party Applications for Educators page on the StaffWeb. Applications that have been reviewed for privacy and security by SCDSB will be categorized as follows:

8.1.1 Reviewed Applications – Not Approved for Use (Prohibited): The digital tool has been reviewed and is not approved and must not be used under any circumstances, regardless of whether consent is obtained or not.

8.1.2 Reviewed Applications – Approved with Informed Notice (restrictions or conditions may apply): The digital tool has been reviewed and is approved for use by educators but may have restrictions or conditions that the educator and/or students must follow. The Digital Tools Informed Notice Statement (APPENDIX A) is to be shared with parents/guardians, along with the Student Information Computing Technology (ICT) Appropriate Use Agreement (FORM A1300-1). The educator must review the Resource Document and follow the instructions provided.

8.1.3 Reviewed Applications – Approved and Informed Consent Required for Under 13 (restrictions or conditions may apply): The digital tool has been reviewed and is approved for use by educators, but may have restrictions or conditions that the educator and/or students must follow. The educator must review the Resource Document and follow the instructions provided. The educator must obtain informed consent for students under the age of 13 using the Informed Consent Use of Third-Party Applications and/or Website (FORM A1350-1).

8.1.4 Reviewed Applications – Approved and Informed Consent Required for Under 18 (restrictions or conditions may apply): The digital tool has been reviewed and is approved for use by educators, but may have restrictions or conditions that the educator and/or students must follow. The educator must review the Resource Document and follow the instructions provided. The educator must obtain informed consent for students under the age of 18 using the Informed Consent Use of Third-Party Applications and/or Website (FORM A1350-1).

8.2 Applications that have not been reviewed by the ECNO for security and privacy, or reviewed by SCDSB may not be used. To request a review, educators must:

8.2.1 Submit a SUPPORTdesk ticket that details information about that application. This information will inform central staff about applications that may require an SCDSB pedagogical and technology review, followed by an ECNO security and privacy review. Please note that the review process is subject to SCDSB and ECNO wait times.

8.3 With the exception of board approved grading tools, staff shall not transmit records of the board. Student work becomes a record of the board once it has an evaluation associated with it.

9. Security/Safeguards

9.1 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.

9.2 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. 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. Employees should not use the same passwords for systems outside of work as they use for work.

9.3 Employees shall register additional authentication methods that will allow for self-service password resets, and multi-factor authentication for situation where enhanced security is required. These additional authentication methods can include a mobile number for text messages, use of an authenticator application on a mobile device, phone number (office or personal), and/or an alternate email address.

9.4 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.

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

10. Employer Access/Expectation of Privacy

10.1 Employees should not expect that their use of SCDSB ICT equipment or accounts is private.

10.2 Employer access to ICT shall be for the following purposes to:

10.2.1 engage in technical maintenance, repair and, management;

10.2.2 meet a legal requirement to produce records including engaging in e-discovery;

10.2.3 ensure continuity of work processes (e.g. employee departs, employee gets sick, work stoppage occurs, etc.); and,

10.2.4 prevent or investigate potential misconduct and ensure compliance with the law.

10.3 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 APM A1350 - Information and Computing Technology - Appropriate Use Guidelines for Employees.

10.4 A search of employee files, records of activities, and related information will be conducted if there is reasonable suspicion that an employee has violated APM A1350 - 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.

10.5 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.

10.6 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.

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

11. Bring Your Own Device (BYOD)

11.1 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 the 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 use a BYOD device, 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.

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

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

11.4 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, April 2019, June 2022, August 2023

Issued under the authority of the Director of Education

Informed Consent
Use of Third-Party Applications and/or Website

___________________________ would like to use the following third-party application or website:
School Name

Name of third-party application(s) or website(s):

We will be using this/these application(s) for the following purpose(s):

Waiver and Release

Yes, I approve of the use □ No, I do not approve of the use □

This/these applications or website(s) may collect personal information (e.g., first/last name, gender, birthdate) for the purposes of providing education and education-related services such as instruction, assessment and evaluation. The collection of personal information is sometimes necessary for us to deliver the services that we are mandated to provide by the *Education Act.* The third-party application(s) or website(s) that are listed on the form are approved for use within the Simcoe County District School Board with consent.

I understand that by giving this consent, I am permitting personal information about me or my child to be used, and further understand that if consent were withheld this use would not occur. I have given this consent voluntarily.

School

Name of student (please print)

Date

Name of Parent/Guardian/Adult Student (please print)

Signature of Parent/Guardian/Adult Student

Witness

Date

Personal information including images and recordings in connection with this form is collected under the authority of the *Education Act* including *s.170, 171, 198, 199, 264 and 265 and* in accordance with the *Municipal Freedom of Information and Protection of Privacy Act* and will be used for promoting, publicizing or explaining the SCDSB and its activities and for administrative, educational or training purposes. Personal information may be disclosed to outside service providers for processing and production. If you have any questions about the collection of personal information please contact the principal of the school or the Controller, 1170 Highway 26, Midhurst, Ontario L9X 1N6, phone (705) 734-6363, ext. 11259.

DIGITAL TOOLS INFORMED NOTICE STATEMENT

1. Definitions and Overview

Personal information – information about an identifiable individual. Examples include a name, unique identifying number or symbol, together with other information about the individual.

Digital Tools – includes software, applications, web services, browser extensions, etc. These digital tools are used to administer educational programs and associated services and to help deliver them in an efficient and cost-effective manner.

The collection of personal information using digital tools is for the purpose of providing education and education-related services such as instruction, assessment, and evaluation, as well as any ancillary and administrative services, such as attendance, transportation, and facilities. The collection of personal information is necessary to deliver the services that we are mandated to provide by the *Education Act*.

Teachers use digital tools to assist with instruction. These digital tools provide platforms and offer parents/guardians tools for engagement. Digital tools are also used to gather student work for assessment of a student's knowledge, learning skills, work habits, behaviour, learning style, learning strengths, weaknesses, engagement, and achievement.

Staff use digital tools to make the management of data more efficient, secure, and to assist with reporting requirements to parents/guardians and the Ministry of Education.

2. Purpose of Third-Party Digital Tools and Examples of Data Collection

The *Education Act* authorizes the board to collect and use personal information to provide the services that are delivered to students and their parents/guardians.

2.1 Board administration, Ministry reporting, and legal requirements to share information with third parties. Examples of this include:

- student registration and class placement;
- parent/guardian and emergency contact information;
- communication tools for school administrative purposes;
- behaviour, safety tracking, and medical plans of care;
- attendance reporting and safe arrival;
- student evaluation tracking and report card programs;
- special education and student services records (Individual Education plans (IEPs), Behaviour Plans);
- student transportation;
- student photos, yearbook creation, etc.;
- tracking the provision of devices and technology to students;
- reporting to the Medical Officer of Health, Ontario Federation of School Athletic Associations (OFSSA), the Ministry of Education and other third-party providers as authorized;
- home to school communication tools, parent/guardian portals, etc.; and,
- payment processing for field trips and lunch programs.

2.2 Student instruction, assessment and evaluation, including remote learning. Examples of this include:

- learning Management Systems (LMS) (i.e., Google Classroom, D2L/Brightspace);
- video conferencing, communication, and collaboration tools (i.e., Google Workspace for Education, Microsoft Teams);
- assessment and evaluation tools; and,
- digital portfolios (i.e., myBlueprint, portfolio).

2.3 Education tools to support content creating, collaboration, communication, critical thinking and organization. Examples of this include:

- coding programs;
- blogging;
- digital math tools;
- music programs;
- video and music editors;
- organizational tools; and,
- digital reference library database.

2.4 Experiential Learning. Examples of this include:

- simulations;
- digital field trips;
- guest speakers; and,
- cooperative education.

3. Legal Requirements for the Collection, Use, and Disclosure of Personal Information

The *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* regulates how a school board collect and manage personal information.

3.1 Authority to Collect Personal Information:
The *Education Act* and Ministry of Education provide the authority for school boards to collect personal information about parent/guardian and students enrolled in school.

3.2 Notice of Collection:
This notice is required to advise you that we will be collecting personal information belonging to students and their parent/guardian to provide educational services. A copy of this notice is available on the board website by following this link. Additionally, this link outlines how the board uses digital tools to fulfil its objectives.

3.3 Use of Personal Information:
The Simcoe County District School Board (SCDSB) will only use the personal information collected for the reason it was collected, for a purpose that is consistent with why it was collected, or with consent, use it for a different reason.

4. Disclosure of Personal Information

The SCDSB will only disclose the personal information collected for the reason it was collected, or for a consistent purpose that is necessary and proper to provide educational services.

In some cases, the board may disclose personal information to digital tool providers as agents, and they might be kept to collect, use and/or retain personal information on behalf of the board for the board's purposes. In such cases, the digital tool providers are providing the board with services to fulfil the board's mandate and in a manner that meets the board's legal responsibilities and policy requirements.

When personal information is disclosed to digital tool providers, the board retains ownership and control of the personal information. The providers are only permitted to use the information to provide services for the board and the digital tool providers must ensure that the personal information is secure from unauthorized access, use or disclosure.

5. Protection of Personal Information

Reasonable security measures must be used to protect personal information from inadvertent or unauthorized access or disclosure.

5.1 only those individuals who require access to information to fulfil their job or contractual duties can have access;
5.2 service providers cannot directly or indirectly disclose, sell, share, destroy, exploit, or use any personal information (except as permitted by law); and,
5.3 industry standard security measures are required to be used to protect personal information.

6. Risk Mitigation Strategies to Protect Personal Information

The board has policies and procedures that provide guidance for staff and service providers regarding when and how they can use digital tools that collect personal information.

Strategies are used, when possible and appropriate, to prevent the collection of personal information that is not needed for the board's purposes. Examples include using teacher generated codes, pseudonyms, or anonymous user accounts and/or minimization of personal information collected by the digital tool.

Any questions regarding how the board collects, uses, or discloses personal information may be referred to the school principal or the SCDSB Controller. Questions on the board's use of digital tools, or a particular digital tool used in the classroom can be directed to the classroom teacher, school principal, or the Student Achievement department at digitallearning@scdsb.on.ca.