Simcoe County District School Board

STUDENT INFORMATION COMPUTING TECHNOLOGY 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, 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/student's acknowledgement and agreement of the appropriate use is required annually. Digital media learning environments use ICT to help students to communicate and work collaboratively, and support individual learning and contribute to the learning of others while gaining skills required to being productive and safe digital citizens. Students use a variety of applications which may include blogs, wikis, learning management systems (such as Moodle, Desire 2 Learn, 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 appropriate use agreement with students at the start of the 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 focused, 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 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.

Simcoe County District School Board

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).
- use ICT to record or photograph other students 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 your child'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 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 wireless guest networks 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/legal 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.

How to log on to the school computers:

You will be required to change your password the very first time you login. Shown below is a sample login for a fictional student named Ann Jane Doe.

- First four letters of the student's name, the last three digits of their eSIS number and a 0,1,2, etc. If there are less than four letters in the student's first name we continue using letters from their middle name until the four letters are reached (e.g., "annj7890").
- The initial password created for secondary students is their birth date in the following format: YYYYMMDD. For example, Ann Jane Doe's birthday is November 21, 1987, which makes her initial password 19871121.
- Therefore, Ann Jane Doe's username and initial password are: Username: annj7890
  Password: 19871121

If students do not hand in their signed Responsible Use Policy for the Use of Computers by September 16th, they will no longer be able to log on to the computers.