ST. CLAIR CATHOLIC DISTRICT SCHOOL BOARD
POLICIES AND PROCEDURES
SECTION B: ADMINISTRATION

RESPONSIBLE USE OF TECHNOLOGY	PROCEDURE
EFFECTIVE: 2013 04 23	

ADMINISTRATIVE PROCEDURES:

1.0 Responsibility

1.1 Department managers and principals will annually review the policy and related procedures with their staff and school community councils, prior to the end of September.

1.2 The Manager of Human Resources (or designate) will provide to all new staff a copy of the Responsible Use of Technology policy as part of their staff orientation program. New staff will be required to acknowledge, in writing their agreement to comply with this policy and related procedure.

1.3 Principals will provide to all new students and their parents/guardians a copy of the policy and related guidelines upon enrolment with the Board.

1.4 Principals will ensure that, at the commencement of each school year, teaching staff review the policy and related procedures with their students and communicate to the parents/guardians the Board's expectations with respect to the subject matter of the policy.

1.5 Teachers will review the expectations of this policy and guidelines with their students at the beginning of each school year and throughout the year, as may be necessary, to ensure that the policy and the procedures are being followed.

1.6 Network/internet users are responsible for appropriate, legal, moral and ethical behaviour when using the Board's networks either through Board-owned or personally-owned electronic devices (PEDs). Access to network services is a privilege granted to responsible users. Inappropriate use of the networks or equipment may result in a suspension or cancellation of access privileges.

1.7 PED users accessing the Board's networks may be required to acknowledge and agree electronically to the provisions of this policy and must have and maintain updated anti-virus software on their equipment, as applicable. A diagnostic confirmation for compliance may be conducted on a PED with each attempt to sign-in to the Board's network.

1.8 Superintendents, principals and managers, or designates, have the right to ban any or all PEDs on Board property and at Board events.

1.9 Staff, students and visitors will use PEDs in accordance with all policies of the Board. Any person who opts to utilize their PED while on Board-owned premises, during Board-related excursions or functions do so at their own risk. The Board will not be responsible for any damage or theft to any PED and will be held harmless under the terms of this policy.

1.10 Teaching staff have the right to determine how and when technology will be used by students during instructional periods, regardless of the ownership of the device.

1.11 The Board assumes no responsibility or liability for any phone usage or other charges, costs or fees of any kind or nature whatsoever, or for any damages that a user may incur or suffer when PEDs are used to access the Board's network. This includes the loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions. No technical support will be provided for PEDs by Board staff.

1.12 The Board makes no representations, warranties or conditions of any kind, whether expressed or implied, for the network service it provides.

1.13 Use of any information obtained via the Board's network, including the internet, is at the user's own risk.

1.14 Network users may not willfully access any files or content that may damage, compromise, violate, infiltrate or in any way negatively affect Board electronic devices, hardware, software, networks, directories and files or those of other users.

1.15 Network users will immediately notify the HelpDesk or their teacher if their password is lost or stolen or if they have reason to believe that some person has obtained unauthorized access to their Board network account.

1.16 Network users must immediately notify their teacher/principal/manager or supervisor if they are aware of any inappropriate use of information or communications technology.

a) The principal/manager must notify their supervisory officer of inappropriate conduct immediately where the incident involves a staff member.

b) The supervisory officer will determine if Information Services staff should be notified and directed to alter network access before any action is taken.

c) The appropriate supervisory officer or designate will determine whether disciplinary action is warranted for staff.

d) The principal must notify the student's parent/guardian of the inappropriate conduct immediately, when the incident involves a student.

e) The school principal or designate will determine whether disciplinary action is warranted for students.

1.17 The Board has the authority to monitor and manage all accounts and network activity. Access or bandwidth usage may be denied as deemed necessary to ensure the integrity of the Board's systems without notice.

1.18 Changes in networks or equipment location within schools will be determined in conjunction with Information Services staff. Schools wishing to relocate equipment will make a request to the manager responsible before proceeding. Costs related to such initiatives undertaken by schools without prior consent will be borne solely by

the school up to and including costs incurred to reverse the change made by the school.

1.19 Principals will be responsible for seeking restitution from students and/or parents/guardians when Board-owned electronic equipment is willfully damaged or stolen.

2.0 Expectations

2.1 The Board will provide all permanent staff user account access to a computer network to permit them to efficiently fulfill their responsibilities as assigned by the Board in support of its mission and goals. The person to whom an account is issued is responsible at all times for its proper use.

2.2 Board-provided user accounts, hardware, software and network services shall only be used for intended instructional, educational or administrative purposes. Commercial activities for personal gain by students, visitors, staff or former staff are not permitted using these resources.

2.3 The standards of behaviour as outlined in the Provincial Code of Conduct apply to all members of the school community who access the Board network or who use personal or Board-owned devices while on Board property, or to conduct Board-related business or Board activities on or off Board property (i.e. field trips, sports events, etc.).

2.4 Cyber bullying is strictly prohibited.

2.5 PEDs owned by staff, students, volunteers or visitors must only be used in ways which are consistent with the vision and mission of the St. Clair Catholic District School Board and as outlined in 2.3 above.

2.6 Staff must maintain proper professional boundaries when using social media/networks and any form of electronic communication.

2.7 The Board does not permit the access or use of internet sites that contain inappropriate, offensive, or illegal content.

2.8 Network users will conduct themselves in an ethical manner and are not permitted to transmit, request, submit or publish any defamatory, inaccurate, abusive, obscene, profane, pornographic, threatening, harassing, offensive, racist, illegal or any other inappropriate material, regardless of ownership of the equipment or network being used.

2.9 All network users will ensure that all communication is in compliance with privacy legislation, and that all records in the custody and control of the Board that contain personal information that pertains to a student or other individual will be held in strict confidence.

2.10 Network users must respect copyright laws and licensing requirements that protect software owners, artists, writers, and other creators. The number of Board-owned legally permitted software licences must not be surpassed and cannot be installed on PEDs. Information and media protected under copyright laws can only be used, sent or received with appropriate permissions. Violations of this requirement will result in removal of the illegal software and may result in a loss of network access privileges.

2.11 Network users are prohibited from accessing, using or uploading onto the Board's network or onto any hardware, from any other source, or downloading onto the Board's network from any source, any software other than that which is approved and properly licensed.

2.12 Network users are prohibited from conducting activities that are wasteful of network resources or that degrade or disrupt network performance. Such activities include, but are not limited to, unauthorized online games, "broadcast" messages and "chain letters". Any damage resulting from such behaviour shall be deemed to be the responsibility of the user and/or parent or guardian.

2.13 E-mail correspondence will be conducted and abide by the generally accepted rules of network etiquette, otherwise known as netiquette. (See definition in 5.0)

2.14 Using someone else's password or accessing the private electronic or private online content of other users without consent is prohibited. Sharing passwords with others is strictly prohibited.

2.15 Board staff shall not contact or interact with students through their personal email or social network accounts or through the student's personal accounts unless the student is a member of the staff member's immediate family. Staff will conduct themselves in a manner that is compliant with all Board policies and with the Ontario College of Teachers' Ethical Standards as applicable. (See 4.4 for link)

2.16 Unless given written permission from a principal or supervisor, staff members are not permitted to establish and use social network sites to speak on behalf of the school, department or Board. When permission has been granted, staff will use their own name when participating on-line and will do so in an environment that can be monitored by the Board.

2.17 Unauthorized access by any user of another individual's electronic information is a violation of the policy. Access by a user of another individual's electronic information will only be permitted with the written approval of the superintendent responsible for the information technology department or his/her designate.

2.18 Each network user recognizes that users do not have a reasonable expectation of privacy with regard to the use of voicemail, email, intranet and internet usage, even when this use is restricted to Board business and the information is stored on its computers.

2.19 The Board has the right to inspect any computer or computer systems and to monitor the use of technology, including, without limitation, inspecting the contents of voicemail and email messages. Users will not necessarily be notified when such monitoring is to take place, or whether monitoring has occurred. In certain situations, the Board may be compelled to access, read, copy, reproduce, print, retain, move, store, destroy and/or disclose messages, files or documents stored or sent over its email, internet or computer systems. These situations may include the following:

a) in the course of regular maintenance of a computer;
b) in the event of a request for documents as part of a litigation or similar proceedings; or
c) where the Board has reason to believe that the computer system is being used in violation of the policy.

2.20 When there is reasonable cause to suspect inappropriate conduct or illegal acts through the use of the Board's networks, further investigation may be required. Consent by any two of the following three persons is required before an investigation into the email account or personal network drive of the user can be conducted.

a) Director of Education
b) Senior Business Official
c) Chair of the Board

2.21 Users of Board-owned portable electronic devices are expected to take reasonable measures to secure the devices at all times.

2.22 Students will inform their teacher and staff will inform their supervisor of damage or theft of Board-owned technology equipment promptly. The school principal or departmental manager will inform the manager responsible for Information Services of the damage or theft which will then arrange for replacement of the device if possible or reasonable.

2.23 A supervisory officer will determine appropriate disciplinary action, if any, including restitution, when Board-owned technology has been damaged and/or stolen.

2.24 Willful or malicious damage or theft of Board equipment, networks or software shall be deemed the responsibility of the person(s) responsible and/or parent or guardian. Malicious damage includes, but is not limited to, physical damage to hardware or deliberate introduction of a virus or noxious program.

2.25 School or department staff will complete a HelpDesk request only for Board-owned electronic equipment that requires repair and will do so in a timely manner. Students and staff are not to address hardware or software problems without the direction of Information Services staff.

2.26 Devices with camera, audio or video recording capabilities are absolutely prohibited in areas where there is an increased expectation of privacy (i.e. change rooms, restrooms).

2.27 Students must obtain permission from staff prior to the use of devices noted in 2.26.

2.28 The Board is required to protect the privacy of its students. Personal information should not be published without the informed consent of a parent/guardian. For students 18 years and older, or for those students that have withdrawn themselves from parental care, the students' informed consent is required.

2.29 Violation of the Responsible Use of Technology policy may result in restricted network access, loss of network access, liability for the cost of remediation and/or, disciplinary action up to and including dismissal in matters concerning staff; and disciplinary action up to and including suspension and/or expulsion in matters concerning students. Legal action including, but not limited to, criminal prosecution under appropriate provincial and federal laws, may also be initiated.

3.0 Appropriate Use of Technology

Without limiting the generality of anything in this policy, each network user shall use technology in a manner consistent with the Board's values, and in an ethical and lawful manner. Examples of conduct that violate the policy are as follows:

a) using Board technology to create, possess, distribute or access illegal, offensive, pornographic and/or inappropriate materials;

b) sending or willingly receiving messages which are defamatory, abusive, obscene, profane, threatening, racially offensive or sexual in nature;

c) downloading, storing or sharing illegal, inappropriate, offensive or obscene material on Board-owned computer systems;

d) downloading, storing or sharing on Board-owned computer systems media files, including music and video files that are illegal, offensive, obscene, inappropriate or that are not intended for Board purposes;

e) downloading, installing or sharing unauthorized or improperly licensed software;

f) knowingly accessing sites containing sexually explicit, racist, homophobic or other material clearly inappropriate in a school or work environment;

g) uses that are malicious, unethical or in violation of accepted community standards and/or Board policies;

h) uses that violate any federal or provincial laws;

i) knowingly creating, exchanging, transmitting and/or downloading messages or data that are offensive, harassing, obscene, libelous, abusive, discriminatory, or threatening or that encourage violence;

j) conducting business activities which are unrelated to the user's duties and responsibilities to the Board;

k) advertising or soliciting, including advertising of personal services;

l) attempting to access another person's account or private files or misrepresenting one's self as another person in electronic communications;

m) sending or forwarding anonymous or inappropriate unsolicited email messages, including mass email messages, such as chain letters, jokes or spam;

n) computer-hacking and related activities; and/or

o) attempting to disable or compromise the security of information contained on Board computer systems.

4.0 Additional Information

4.1 The Board is committed to the principles of equity and inclusive education, consistent with our Catholic teachings, which value and promote human rights and social justice in all Board policies, programs, guidelines, operations and practices.

4.2 Ministry of Education Policy/Program Memorandum No. 128, the Provincial Code of Conduct, and the St. Clair Catholic District School's Board Code of Conduct give direction regarding responsibilities outlined under subsection 301(1) of Part XIII of the Education Act and establish expectations "governing the behaviour of all persons in schools". These expectations will govern the use of technology as per the following link: http://www.edu.gov.on.ca/extra/eng/ppm/128.html

4.3 Reference materials regarding appropriate electronic communication guidelines for staff can be obtained by referring to *Cybertips for Teachers*, an information brochure published by the Canadian Teachers' Federation.
http://www.ctf-fce.ca/Documents/Resources/en/cyberbullying/2011/CYBER2011_Brochure_EN_PRINT.pdf

4.4 Ontario College of Teachers' Ethical Standards for the Teaching Profession can be viewed at the following link: http://www.oct.ca/standards/ethical_standards.aspx

4.5 Ontario College of Teachers' Professional Advisory: Use of Electronic Communication and Social Media can be viewed at the following link:
http://www.oct.ca/resources/advisories/use-of-electronic-communication-and-social-media

5.0 Definitions

Cyber bullying: bullying by electronic means, including:

a) Creating a web page or a blog in which the creator assumes the identity of another person;
b) Impersonating another person as the author of content or messages posted on the intranet/internet; and
c) Communicating material electronically to more than one individual or posting material on a website that may be accessed by one or more individuals. (Policy/Program Memorandum No. 144, released by the Ministry of Education, December 5, 2012)

Devices: references to electronic devices include current and emerging technologies such as netbooks, notebooks, desktop computers, tablets, iPads®, iPods®, cameras, cell phones, smart phones, BlackBerry®, audio/video equipment, copiers and all other devices that are capable of recording, storing, processing, communicating and/or transmitting information, images or sound digitally.

Informed Consent: means consent provided by an individual after he or she has been made aware of exactly how information, including images, school work, etc., may be collected, used or disclosed including where it will appear and for how long. Informed consent provides as much information as possible.

Network: means the Board's technology networks and includes all related systems.

Network Users: includes trustees, administrators, academic and support staff, students and parents, visitors, volunteers and persons associated in any way with the St. Clair Catholic District School Board.

Netiquette: a protocol of accepted and approved customs for technology users, which includes but is not limited to the list below. Users must:

a) be polite in all communications;
b) use appropriate language (no profanity, bullying, harassing or threatening language);
c) be cautious in giving out personal information, whether of the user's or of any other person;
d) **not** use the Network in such a way that you would disrupt the use of the Network by other users;
e) **not** include any inappropriate information or confidential information in email communication whether of the user's or of any other person;
f) **not** make or transmit any communication in contravention of applicable laws (e.g., copyright, privacy, anti-spam); and
g) **not** transmit any files, information or materials designed to tamper with data or Networks maintained by the Board or any other person.

Personal Information: includes all images, including photographs, digital images, postings on the Internet, films, and video recordings, as well as an individual's name, address and school work.

PED: a personally-owned electronic device.

Social Network: an electronic community maintained on websites and accessed through the Internet or through web-based accounts or other type of internet account. (A social Network does not include any school or Board related site, wiki or blog approved by the Principal)

Staff: includes principals, teachers, supervisors, superintendents, managers and other employees of the school or the Board.

Appendix A

ST. CLAIR CATHOLIC DISTRICT SCHOOL BOARD

STUDENT GUIDELINES FOR RESPONSIBLE USE OF TECHNOLOGY

The Board recognizes the important role of information, collaboration and communications technology in helping students to research, collaborate, learn and communicate. Access to Network services through board-owned and personally owned equipment is a privilege granted to responsible users. The Board requires that the use of technology in its schools, offices and during educational excursions be conducted in a responsible manner, regardless of device ownership as per *Sec. B. Policy – Responsible Use of Technology*.

This requires that students are ethical, appropriate, legal and moral and use technology in ways that are consistent with the teachings of the Catholic Church and the Board's Belief Statements.

All users of technology should:

a) respect and protect themselves;
b) respect and protect others; and
c) respect and protect intellectual property and technological property.

Students may not:

a) use technology without staff direction or supervision;
b) share their login or password;
c) access, change or delete files or data that they do not own;
d) access or use internet sites that contain inappropriate, offensive, or illegal content;
e) attempt to intentionally misuse, damage or repair** networks, servers or computer equipment;
f) download or install software, regardless of device ownership;
g) use inappropriate language (no profanity, bullying, harassing or threatening language);
h) conduct or participate in cyber bullying or any deliberate activity intended to hurt or harm others;
i) use technology for the promotion or execution of illegal activities;
j) create or transmit communications that would violate copyright or other applicable laws; nor
k) generate, communicate or transmit any inappropriate or confidential information or images using technology.

The Board has the right to monitor information and data regardless of device ownership when that device is using Board-owned technology and/or networks. Personal use of Board-owned equipment and networks is prohibited.

Use of personal electronic devices (PEDs) by students is permitted as authorized by Board staff and requires written parental/guardian consent. Acknowledgement of the Board's Responsible Use of Technology policy may be required upon logging on to the Board's networks.

The Board assumes no responsibility for the safe-keeping of PEDs brought to school, for usage fees that may be incurred when used in schools or for their maintenance and support. Any damage to or theft of personal equipment is the sole responsibility of the owner.

Devices with camera, audio or video recording capabilities are absolutely prohibited in areas where there is an increased expectation of privacy, such as change rooms and restrooms. Audio recordings and photos of students or staff are not permitted without appropriate prior consent.

Violation of these expectations may result in:

a) restricted network access;
b) loss of network access; and/or
c) disciplinary and/or legal action.

** Except for curriculum-related purposes under direct staff supervision