HURON-PERTH CATHOLIC
District School Board

Information and Communications Technology

Adopted:	**August 30, 1999**	**Policy #:**	**3.2.1.**
Revised:	**October 23, 2023**	**Policy Category:**	**3.2. Information and Communications Technology**

BELIEF STATEMENT:

The Huron-Perth Catholic District School Board (the Board) believes that appropriate use of all information and communication technologies must reflect Catholic teaching and support the academic, cultural, and spiritual growth of students. As a Catholic learning community, we commit to using these and all technologies in a manner which is consistent with Catholic Social Teaching.

POLICY STATEMENT:

It is the policy of the Board to provide a principled framework for the effective use of technology in a manner which complements, enhances, and achieves the educational objectives of our Catholic School District.

PROCEDURES:

1. **General**

   The Board will provide all schools with hardware, software and networking capabilities to support effective instructional practices for teaching and learning. Any hardware or software requested by individual schools must first be approved by the ICT Manager and IT Learning Coordinator and be compatible with the existing School Board technological, cyber-security and privacy infrastructure. Application for approval via the prescribed form.

2. **Requirements for Appropriate Use**

   Principals will ensure that teachers review the following requirements for appropriate use and share applicable information with their students at least once per year.

   2.1 Use of Board Digital Technology

   The Board provides digital technologies to students and staff for the sole and limited purposes of achieving the educational goals set out in this policy statement and the Board strategic plan and Ministry Curriculum. Recognizing the value and contribution that digital technologies provide, it is the intention that students will use these resources wisely and only for the stated purposes of their studies.

   Security of any computer system is a high priority, especially when the system involves many users. If a potential security problem is identified, an immediate supervisor,

teacher or ICT must be notified.

2.2 Full-Length, Feature Film Usage

The Board does not support the use of full-length feature films as a classroom learning activity. We embrace pedagogical practices that nurture critical thinking in accordance with the policies and constructs of Growing Success, Ontario Ministry of Education.

2.3 Network Usage

Students and staff have an obligation to access and use the Board's network responsibly and with regard to others' privacy and others' rights. Students and staff have an obligation not to intentionally compromise the integrity or operation of the Board's network and technology infrastructure.

Users shall not directly or indirectly or from any source whatsoever:

- Tamper with, willfully access and/or modify system data, data containing confidential information, or other data for which they have not been given access;
- Use/change logins other than their own;
- Conduct activities that might be detrimental to the integrity of the Board's network;
- Conduct activities that are wasteful of network resources or that degrade or disrupt network performance.

2.4 Internet Usage

Students and staff have an obligation to use the Board's network facilities to access and/or transmit information through the Internet in a responsible manner. Anyone using the Board network must do so in accordance with the beliefs of this policy statement.

The Internet is recognized as an essential tool for learning. Blended learning (i.e. the use of a learning management system and/or digital online tools) are central to the strategy that aims to:

- Improve communication between the teacher and students;
- Promote greater collaboration and critical thinking among students;
- Differentiate learning and assessment for all students;

To ensure that all students have access to these services, student information may be used in the setup and tracking of accounts of Ministry or Board endorsed online programs.

2.4.1 Students and Staff:

Students and staff shall <u>not</u> use the Board's digital technologies in a manner, which compromises the provisions of this policy statement.

Students and staff shall <u>not</u> access and/or transmit or attempt to access and/or transmit any of the following information through the Internet or upload onto the Board's network or onto the hard drive and/or cloud storage of any Board-owned device in the school, from any other source, or download onto the Board's network from any other source any software other than Approved Software:

- Any files, information, materials, or communications containing Inappropriate Information or Confidential Information (other than Confidential Information

relating solely to the user);
- Any files, information, materials, or communications which are designed to tamper with or have the potential to facilitate the tampering with the data or networks maintained by the Board or any other person;
- Any files, information, materials or communications, the access to transmission of, or use of which would violate copyright or licensing restrictions associated with such files, information or materials.

2.4.2 Students

All students using Internet access will:
- Act as witnesses to the truth and values of the Catholic faith reflecting the school's Code of Conduct.
- Obtain permission from their teacher before accessing the Internet.
- Download programs only with teacher permission and scan downloaded programs for viruses.
- Back out of any site which is transmitting unacceptable information or graphics and notify their teacher.
- Use proper, socially acceptable language.
- Properly footnote and include in a bibliography any information which is obtained from the Internet and incorporated into an assignment.
- Have access to software platforms such as those provided by the Ministry of Education (provincially funded Virtual Learning Environment), and those approved by the Board (e.gi.e. Google Workspace-Suite for Education) as directed by their teacher.

Students will not:
- Send or display any offensive pictures or messages.
- Use obscene language, or language reflecting prejudice connected to racial, ethnic, religious, sexual orientation and/or gender identity.
- Use the Internet for product advertisement, commercial or for profit purposes.
- Violate copyright laws.
- Use someone else's password or email address.
- Violate security systems, which have been put into place to protect computers, file servers, networks and users, both within and outside the Board.
- Provide personal information about themselves or others through the Internet (name, phone number, address, etc.).
- Put themselves at risk of personal harm as a result of Internet contact
- Contact individuals outside of our school board without the consent and knowledge of their teacher.
- Use Internet access in any way, which is a waste of finite resources.
- Engage in any form of cyberbullying.

The school principal has the right to suspend any user's access to the Board's computer hardware, software, or connectivity for a period to be determined by the principal in the event of a breach of this policy. The failure of a student to comply with this policy statement shall be dealt with in accordance with the Student Behaviour, Discipline and Safety Policy and the School Code of Conduct.

At the beginning of each school year, the prescribed Assumption of Responsibility form is made available to parents/guardians. To post student work or photos on the Board and school website and/or social media sites, the

completed Assumption of Responsibility form must be maintained and will serve as a signed parental/guardian consent form, and will be retained in the school.

Students will also consent to an Acceptable Use Agreement via the prescribed form.

2.5 Electronic Communications

2.5.1 Appropriate Electronic Communication Guidelines for Staff

All employees will use technology in a professional manner and are expected to model ethical and appropriate internet conduct. Staff participating in school-related social media groups should read and adhere to the Ontario College of Teachers Professional Advisories “Maintaining Professionalism - Use of Electronic Communication and Social Media” and “ Video Conferencing Guidelines”.

2.5.2 Staff-Student Online Correspondence

Online correspondence between staff and students must be related to course work, or school-sanctioned clubs/activities:

- Principals will only approve school-based social media groups that include a staff member advisor;
- All school-sanctioned social media groups must adhere to regular school code of conduct practices;
- All school-sanctioned social media groups must have at least two staff members with administrative privileges;
- Teachers participating in school-created social media groups with students must adhere to the ethical standards for the teaching profession at all times, whether in a traditional school environment or an online environment.

Whether communicating with students or staff within the Board or with any other person, users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

- Communicate in accordance with the Catechism of the Catholic Church and Catholic Social Teachings;
- Be polite in all communications;
- Use appropriate language;
- Report incidents of cyber-bullying to a trusted adult (parent, teacher, principal);
- Be cautious in giving out personal information;
- Do not use the network in such a way that you would disrupt the use of the network by other users;
- Do not include any inappropriate information or confidential information (other than confidential information relating solely to the user) in email communication;
- Do not make or transmit any communication in contravention of applicable laws nor shall users transmit any files, information, or materials designed to tamper with data or networks maintained by the Board or any other person; and
- Students and staff should be aware that the Board cannot guarantee that electronic communications transmitted through or pursuant to its network shall remain private and confidential. While not absolutely prohibited, the

Board encourages students and staff to use private computer facilities to conduct non-board or communications of personal nature.

2.6 Personal Devices and Bring Your Own Devices (BYOD)

Bring your own device (BYOD) refers to technology models where students, staff or guests bring personally owned devices to school for the purpose of learning. A personally owned device is any technology not owned by the Board on school board property.

- Personal communication devices owned and/or carried by students may only be used during instructional periods for reasons outlined in the board's code of conduct. This means that use must be for approved educational or medical use only. It must be at times and in locations as determined and permitted by the school principal and/or teacher.
- Personal communication devices may not be carried or be in the possession of students during examinations or during other occasions specified by the teacher or principal.
- The use of personal devices are absolutely prohibited in areas where there is an increased expectation of privacy (e.g., washrooms, change rooms). The taking of photographic images of a person or persons, on school property, at school events, and during school activities and/or hours, is prohibited without the permission of the person or persons being photographed and the principal or designate.
- The electronic transmission or posting of photographic images, audio, and/or video by students of a person or persons on school property, at school events, and during school activities and/or hours, is prohibited without the permission of the person or persons being photographed, the principal or designate, and where the student is below the age of 18, the consent of the parent/guardian. The principal and/or teacher may record photographic images, audio, and or video for the purpose of pedagogical documentation and improved student learning.
- The school principal has the right to ban any or all personal devices on school property, at school events, and during school activities, for some or all students.

2.7 Supervision

The principal and teacher(s) concerned will ensure reasonable and appropriate supervision and use of digital technologies and the Board's digital infrastructure. Users are ultimately solely responsible for their use or misuse of personal devices and of the Board's digital technologies and digital infrastructure. The Board shall not be liable for any claim, loss, or damage suffered or alleged to have been suffered by any student or staff member using or misusing either personal devices or the Board's computer facilities. The Board shall assume no responsibility and shall not be liable in any respect for any claim, loss, or damage suffered by any third party relating to a student's or staff member's use or misuse of personal devices or the Board's computer facilities.

2.8 Failure to Comply with Policy

Students and staff should be aware that certain breaches of these procedures may constitute an offence under Canada's *Criminal Code* and other applicable legislation. Where appropriate, offences of this nature shall be reported to the police and will be dealt with accordingly.

3. School Websites and/or Social Media Sites:

School websites and/or social media sites introduce external visitors to the school's presence, location, purpose, organization, curriculum activities, and interests. The content of all school websites and/or social media sites must be consistent with the Vision, Mission, and Strategic Plan of the Board and be approved by the principal prior to posting.

3.1 Content Standards:

- Concern about the content of any page(s) created by students or staff should be directed to the Principal of that school.
- There must be a link back to the Board's website homepage on the first page of the submission using the Board logo as the icon to identify the link.
- Schools must assume the responsibility of keeping information accurate and current
- All web pages/and or social media sites must include an email address or inquiry form, directed to the principal/designate for any correspondence to the school.
- Web pages must not contain any commercial or promotional advertising beyond advancing the presence of the school on the Internet. It is acceptable for the website creator to be acknowledged.
- School website / social media must not use copyrighted materials without permission.

3.2 Subject Matter

All subject matter on social media/web pages should relate to curriculum instruction, school-authorized activities, and general information that is appropriate and of interest to others.

3.3 Quality

All social media/webpages should be free of spelling and grammatical errors. Documents may not contain objectionable material or point (link) to objectionable material.

3.4 Ownership

Subject to the rights of contributors, if any, to works contributed to a school site, the website and all of the files, information, materials, graphics, photographic or other images, logos, trademarks, trade names, and any other intellectual property whatsoever featured on or incorporated in the web site shall be the sole and exclusive property of the Board. Schools cannot use copyrighted material on the website without written approval by the source.

3.5 Security and Privacy

All social media/webpages must be consistent with the Freedom of Information and Protection of Privacy Policy.

- No school page/social media content should provide the means for people to contact any student directly. If communication back to the school is needed, it should be directed to the principal/designate.
- When using photographs of persons on the school website or social media sites, the school must obtain authorization from the parent/guardian on the Board's prescribed Consent and Acknowledgement form.

3.6 Technical and Design Standards

- All school websites will be located on the Board's web server or a server authorized by the Board.
- Documents/links should be thoroughly tested before and after posting to ensure functionality.
- Final decisions regarding access to active web pages for editing content or organization will rest with the principal.

4. Electronic Social Media:

4.1 Prohibited Communications on Social Media

- Staff are not authorized to communicate on social media on behalf of their school, their department or the Board unless given prior written permission by their principal or supervisor;
- If staff post comments on personal social media sites or public social media sites, they must clearly state that they are not representing the views of their school, their department or the Board.

4.2 Respect, Privacy and Confidential Information

Board staff will not disclose confidential student information or confidential school, department, or personnel records without first obtaining written consent from the principal, supervisor, or guardian for students under the age of 18 or from students aged 16 or 17 who have removed themselves from parental control.

- Board staff will not post communications on electronic social media sites which defame students or Board employees or which denigrate Board policies or procedures;
- Board staff will not engage electronically in behavior or comments that would reflect negatively on the school or Board's reputation;
- Staff must refrain from social media comments and posting, whether personal or school/Board related, that will result in a disruption to the school or Board environment; or negatively impact the staff's ability to perform his or her duties;
- Board and school logos will not be used without first obtaining permission from the school principal or supervisor;
- Board staff will use only their own name, when participating in an online social media group for academic purposes;
- Board staff will ensure that their online comments are respectful of Catholic values and adhere to the procedures as outlined in the Equity and Inclusive Education Policy;
- Board staff must refrain from electronic commentary, content, or images that are defamatory, pornographic, harassing, or that create a negative work environment;
- Board staff may use the Board network to access social media sites that are work-related. Where staff access personal social media sites during the work day, such access must not impede their attention to or the efficient performance of their duties.
- Board staff participating in social media activities will respect copyright laws, not only with respect to the content produced on the social media sites but also to the software that enables it;
- Board staff participating in social media activities acknowledge that all information posted to sites is subject to the provisions of the Municipal Freedom of Information and Protection of Privacy Act;
- Principals and other supervisors may monitor employee use of social media and

social networking websites.

DEFINITIONS:

Approved Software - This means software programs approved for use by students and staff within the school by the school board.

Confidential Information - Includes any and all files, information, materials, or communications of a personal or private nature or including information of a private or personal nature including, without limitation, any files, information, materials, or communications which include, convey, or express any information protected by the Education Act, the Municipal Freedom of Information and Protection of Privacy Act or any successor or similar provincial or federal legislation relating to the protection of privacy or students or staff records and information.

Inappropriate Information - Shall mean files, information, materials, or communications including, but not limited to, any of the following:

- Hateful, racist, or discriminatory material related to sexual orientation and/or gender identity;
- Threatening material;
- Gambling or gaming material;
- Firearms and weapons;
- Pornographic or obscene material;
- Material which expresses opinions or beliefs of a personal nature unrelated to the educational objectives referred to in this policy statement;
- Commercial advertising or similar material;
- Any material deemed by the Board and/or Principal to fall within one of the categories set out above; and
- Any other material as listed in the Student Behaviour, Discipline and Safety Policy.

Cyberbullying - Involves the use of information and communication technologies such as e-mail, cell phone, text messages, instant messaging, defamatory personal websites, and other social media sites to support deliberate behaviour by an individual or group that is intended to harm others.

REFERENCES:

- Freedom of Information and Protection of Privacy Policy
- Student Behaviour, Discipline and Safety Policy
- Ontario College of Teachers Professional Advisory “Maintaining Professionalism - Use of Electronic Communication and Social Media”
- Ontario College of Teachers Professional Advisory “Video Conferencing Guidelines”

RESOURCES, APPENDICES AND FORMS:

- N/A