HALTON
CATHOLIC
DISTRICT SCHOOL BOARD
CD
SB

Procedure No. VI-62

Use of Technology and Digital Citizenship	
Adopted: April 1, 2019	**Last Reviewed/Revised:** August 26, 2024
Next Scheduled Review: 2027-2028	
Associated Policies & Procedures: **I-43** Use of Technology and Digital Citizenship **VI-63** Social Media **I-02** Records and Information Management **VI-82** Records and Information Management Procedure **I-07** Privacy Protection Policy **VI-81** Privacy Protection Procedure **VI-51** Security Breach Procedure **I-24** Fraud Management **VI-24** Fraud Management **I-36** Trustee Code of Conduct **II-39** Progressive Discipline & Safety in Schools Code of Conduct – Suspensions & Expulsions **VI-44** Progressive Discipline and Safety in Schools **II-40** Bullying Prevention and Intervention **II-45** Equity and Inclusive Education **VI-54** Equity and Inclusive Education **VI-60** Student Groups in Catholic Schools **III-14** Employee Code of Conduct **III-16** Workplace Harassment **IV-04** Loss or Damage to Personal Items **VI-101** Information Security Procedure **VI-102** Hate or Bias Motivated Incidents Involving or Impacting Students **VI-103** Electronic Monitoring of Employees **VI-104** Multi-Factor Authentication for Employees **VI-107** Use of HCDSB Purchased Computing Technology	

Purpose

The purpose of this procedure is to support the application of the Halton Catholic District School Board (HCDSB) *Policy I-43 Use of Technology & Digital Citizenship*.

HCDSB supports the benefits that technology can bring to its daily operating activities and student achievement. All users are required to know and abide by this procedure in order to ensure information technology resources are being used in a responsible, respectful and lawful manner.

Application and Scope

This procedure applies to students, staff, trustees, volunteers, and any individual using HCDSB technology as defined below.

References

College of Early Childhood Educators

Copyright Act

Criminal Code

Education Act

Growing Success

HCDSB Code of Conduct and Standards of Behaviour

HCDSB Multi-Year Strategic Plan

Institute for Catholic Education (ICE)

International Society for Technology in Education (ISTE)

Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)

Ontario College of Teachers

Ontario Human Rights Code

Ontario Safe Schools Code of Conduct

PPM 128 - The Provincial Code of Conduct and School Board Codes of Conduct

PPM 164 – Requirements for Remote Learning

Definitions

Bullying - is behaviour that makes the person being bullied feel afraid or uncomfortable. It can be in the form of unwanted repeated aggression or happen one time. It can be carried out by one person or a group of people.

Repeated bullying is persistent and aggressive behaviour directed an individual or individuals that is intended to cause (or should be known to cause) fear and distress and/or harm to another person's body, feelings self-esteem, or reputation.

Bullying can occur in situations where there are real or perceived power imbalances between individuals or groups, and may be a symptom of racism, classism, homophobia, sexism, religious discrimination, ethnic discrimination or other forms of bias and discrimination. Bullying can also be based on, but not limited to, body size, appearance, abilities, or other real or perceived factors. Perceptions about differences are often based on stereotypes perpetuated in broader society.

A power imbalance may occur between a student and the individual based on factors such as size, strength, age, intelligence, peer group power, economic status, social status, religion, sexual orientation, family circumstances, gender, gender identity, gender expression, race, disability, or receipt of special education.

Bullying can take different forms. These include, but are not limited to:

- Physical**:** for example, hitting, kicking, shoving, damaging or stealing property
- Verbal**:** for example, name calling, mocking, put-downs and shameful, threatening, humiliating or discriminatory comments
- Social/Relational: for example, damaging friendships, spreading gossip, rumours or excluding others from a group including teasing, threatening, and other hurtful acts
- Written: for example, writing notes and graffiti that are hurtful and insulting
- Cyber-bullying: is the act of engaging in bullying behaviours through electronic means such as social media platforms, email, text or direct messaging, digital gaming and/or communication applications. Examples of cyber-bullying may include:
    - sending or sharing hateful, insulting, offensive, and/or intimidating electronic communication or images via text messages, emails, direct messages
    - revealing information considered to be personal, private, and sensitive without consent
    - making and/or engaging, and/or participating in fake accounts on social networking sites to impersonate, humiliate and/or exclude others
    - excluding or disrupting access to, a student on purpose from online chat groups, access to accounts and during digital gaming sessions
    - Increasing the use of digital platforms enhances the threat of cyber-bullying as well as other safety risks.

Bullying, including cyber-bullying, may intersect with other forms of sexual exploitation including, but not limited to, sextortion and the non-consensual sharing of intimate images. Traffickers and other sexual predators are increasingly using fake accounts to pose as acquaintances or friends of children and youth to lure, groom and recruit them into engaging in sexual acts or services. Children and youth who experience bullying are at increased risk for being sex trafficked.

Digital Citizenship - Users recognize the rights, responsibilities and opportunities of living, learning and working in an interconnected digital world, and they act and model in ways that are safe, legal and ethical.

Guest Network (HCDSB-GUEST) - The network that is limited to guests of the HCDSB where a user may access the internet and limited HCDSB technology.

HCDSB Network - The primary corporate network where access to HCDSB technology is restricted to HCDSB students, staff and trustees.

HCDSB Supported Tools - online digital programs for use and supported within HCDSB

HCDSB Technology - Technology resources include, but are not limited to, computers, tablets, phones, cellular/mobile technology, servers, networks, Internet services, printers, peripherals IoT devices (Internet of Things), computer applications, data, email and collaboration tools, as well as approved third-party Internet service providers to HCDSB include E-Learning Ontario and online textbook vendors. The examples of the services they provide are software, virtual learning environments and digital textbooks.

IOT (Internet of Things) - is a system of interrelated computing devices, mechanical and digital machines, objects that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

Personal Mobile Device - refers to any personal electronic device that can be used to communicate or to access the Internet, (such as a cellphone, tablet, laptop or smartwatch).

Social Media - refers to the use of web-based technologies (websites/blogs, platforms and/or applications) that enable users to communicate and share information online.

User - A user is any individual granted authorization to access HCDSB technology, as defined above.

Principles

HCDSB is committed to preparing our students for the workplace and for success in a world that continues to evolve through advances in technology.

Fundamental to student success is the ability to use technology responsibly to gather, evaluate, construct and share knowledge in a 21st Century world. The objective is to develop the HCDSB community as global citizens and 21st Century learners who strive to achieve the Ontario Catholic School Graduate Expectations.

At HCDSB, educators and learners collaborate in innovative school and classroom communities that encourage student engagement, learning and achievement. As such, HCDSB is committed to:

- creating a positive school climate that supports the achievement and well-being of all students and upholds all human rights;
- taking reasonable precautions to ensure that data is secure and safe and should be used for intended purposes only;

- committed to using technology resources responsibly;
- complying with federal and provincial legislation, as well as HCDSB policies and corresponding operating procedures;
- supporting innovative teaching practices and instructional methods enabled by technology to more precisely address the learning needs of all students;
- engaging students in authentic, personalized, relevant inquiry learning;
- modernizing schools and classrooms that support and enhance innovation in learning;
- providing high capacity network infrastructure, software deployment strategies, cloud-based applications;
- mapping the Ontario Catholic School Graduate Expectations to the 21st century (global) competencies;
- providing staff with training and resources to better utilize technology relevant to their learning needs.

Requirements

All users must review and be familiar with HCDSB *Policy I-43 Use of Technology & Digital Citizenship*.

All users must fully respect intellectual property rights including copyright, privacy rights, human rights (including the right of freedom from harassment), defamation, and criminal laws. In addition, users must fully respect Safe Schools policies and procedures, as well as all other pertinent legislation, regulations and policies in force.

All users are responsible for the care and security of HCDSB technology.

All users are required to use HCDSB and/or Ministry of Education supported tools.

All users must not use HCDSB-issued credentials to log into tools or services not supported by HCDSB without approval from the Senior Manager of Information Technology.

All users accept all terms and conditions of the HCDSB network and internet use while on HCDSB property and/or when logging into an HCDSB account.

HCDSB Supported Online Educational Tools

The following tools are supported by HCDSB and/or the Ontario Ministry of Education:

- **Office 365**

  This includes, but is not limited to, programs such as Outlook, Teams, Word, Excel, PowerPoint, Class Notebook, Sway, and Forms.

- **Brightspace D2L** (the Ministry purchased and supported Virtual Learning Environment).

Ministry created course content is available through the D2L platform in addition to a wide variety of tools that assist in assessment, feedback, collaboration, communication, and classroom management.

- **Google Workspace** (Formerly G Suite)

  A secure collaboration and productivity apps for businesses of all sizes. Includes Gmail, Drive, Docs, Sheets and Meet. To request a new digital resource, follow the HCDSB Digital Resource Request Process.

Considerations before submitting a Request for Use of Digital Tools not approved on HCDSB's Digital Resource Registry:

- **Usage:**
  - The pedagogical reason for using the tool.
  - How does the tool enhance learning and support the implementation of curriculum expectations?
  - If students are permitted to use the tool (e.g., verify the age requirements of the digital tool being considered, it is not limited to over 13/18 years of age etc.)
  - There is no current HCDSB or Ministry of Education approved tool that can perform the same task.
- **Student Data:**
  - If the digital tool requires student personal information to create an account, approval is required by HCDSB's Privacy Office.
  - The vendor is willing to sign a data sharing agreement and/or uses a third party to help protect data.
- **Data Ownership:**
  - Do the Terms and Conditions stipulate that the company owns all of the data?
  - Does the company use data for marketing or research purposes and can it do so in perpetuity?
  - What is the company's data retention policy?
- **Corporate Digital Citizenship:**
  - The company keeps data confidential.
  - The company is accountable to a legal body (legal means can be taken if necessary).
  - The company will notify the user if it changes the terms of service or privacy policy.
- **Digital Resource** (e.g. Apps) **Request Process:**
  - All educators must consider the varying factors impacting privacy and security before submitting a request to use an educational tool that is not listed on HCDSB's Digital Resource Registry.

  - Educators must consult with the curriculum consultant for information about the third-party educational tool request process.
- **Overall Considerations:**
  - Informed consent: Educators must obtain informed consent from students' parents/guardians for digital tools as determined by the Manager, Privacy and Records Information Management and/or the Senior Manager, Information Technology.
  - Terms of Use and Privacy Policy: Educators must ensure that they read and understand the terms of service and privacy policy associated with the digital tool.
  - Familiarity with the digital tool: Educators should test the proposed digital tool and feel comfortable with its use for educational purposes.

Responsibilities

Superintendents, Principals and Managers/Supervisors are responsible for:

- ensuring that staff review *Policy I-43 Use of Technology* & *Digital Citizenship*;
- establishing and monitoring digital citizenship and responsibility through the HCDSB Code of Conduct and Standards of Behaviour;
- instructing and modeling, for staff and students, digital citizenship and responsibility;
- ensuring that all communication is in compliance with applicable privacy legislation, and that all records in the custody and control of the HCDSB that contain personal information that pertains to a student or staff member will be maintained in strict confidence;
- reviewing acceptable use of technology and social media with all staff and students;
- ensuring that if an educator wishes to use a tool that is not currently supported by HCDSB and/or the Ontario Ministry of Education, they are required to follow the *Digital Resource Request Process.*
- ensuring through the Senior Manager, Information Technology, that all students are issued an HCDSB network login to support the development of Digital Citizenship and 21st Century Learning. Student accounts will be deactivated upon departure from HCDSB.

Principals are responsible for:

- ensuring that all members of the school community are informed that student use of personal mobile devices during instructional time is not permitted, except under the following circumstances:
  - for educational purposes only, as directed by an educator
  - for health and medical purposes
  - to support special education needs

Educators are responsible for:

- the supervision of student use of technology and personal technology and mobile devices;
- instructing and modeling, for students, digital citizenship, responsibility, and the safe use of technology as referenced in the *Acceptable Use of Electronic Assets* at the beginning of the school year or semester; this includes modeling appropriate use of personal mobile devices.
  - Educators are not to use personal mobile devices during instructional time, unless explicitly for work-related purposes.
- determining when students are able to access HCDSB technology;
- determining the circumstances for student use of personally owned mobile devices, i.e., for educational purposes only; for health and medical purposes; to support special education needs;
- requesting exception approval to access social media platforms using HCDSB technology for pedagogical and/or work-related purposes only;
- requesting exception approval for students to access social media platforms for educational purposes only;
- requiring students to store personal mobile devices out of view and powered off or set to silent mode during instructional time, unless their use is explicitly permitted by the educator;
- in accordance with PPM 128, if a personal mobile device is not stored out of view, require the student to hand in the device:
  - for grade 6 and below: if the educator sees a personal mobile device that is not stored out of view, they must require the device be handed in for the instructional day and the device must be placed, by the student, in a storage area in a location designated by the Principal;
  - for grades 7-12: if the educator sees a personal mobile device that is not stored out of view, they must require the device be handed in for the instructional period and the device must be placed, by the student, in a storage area in a location in the classroom designated by the educator;
- ensuring that all communication is in compliance with applicable privacy legislation, and that all records in the custody and control of the HCDSB that contain personal information that pertains to a student or staff member will be maintained in strict confidence; and
- ensuring that if they wish to use a tool that is outside those supported by HCDSB and/or the Ontario Ministry of Education, they must follow the *Digital Resource Request Process.*

Students are responsible for:

- using HCDSB technology and/or personally owned technology/devices while on HCDSB property under the following circumstances only:
  - for educational purposes only, as directed by an educator
  - for health and medical purposes

    - to support special education needs
- storing their personal mobile device out of view and powered off or set to silent mode during the instructional period/day, except when their use is explicitly permitted by an educator;
- the consequences of not following the HCDSB's policy and procedures on personal mobile device use and social media use;
    - if the student does not hand in their personal mobile device when required, they must be sent to the Principal's office;
- complying with restricted access to social media platforms on school networks and school devices unless directed by an educator for educational purposes
- demonstrating digital citizenship through the appropriate use of technology, as outlined in HCDSB Code of Conduct and Standards of Behaviour;
- reporting any inappropriate use of email, data, or unauthorized technology to an educator or administrator immediately;
- the care, maintenance and security of their personal electronic devices – the HCDSB is not responsible for the replacement of lost, stolen or damaged items.

Remedial Practices and Progressive Discipline

Individuals who do not comply with *Policy I-43 Use of Technology & Digital Citizenship* will be subject to appropriate consequences consistent with HCDSB policies and procedures related to Codes of Conduct, progressive discipline and the Education Act.

Principals will consider a range of interventions and progressive discipline to address student behaviours within the Education Act and *Policy II-39 Progressive Discipline & Safety in Schools Code of Conduct – Suspensions & Expulsions*.

Consequences may include, but are not limited to, the following, either singularly or in combination depending on the individual circumstances:

- limitations, suspension and/or revocation of access privileges to personal and HCDSB technology resources;
- for staff, appropriate disciplinary measures, up to and including termination for just cause;
- referral to relevant authorities (e.g., police).

APPROVED: Regular Meeting of the Administrative Council

AUTHORIZED BY: ________________________________

Director of Education and Secretary of the Board