Huron-Superior Catholic
DISTRICT SCHOOL BOARD

ACCEPTABLE USE OF INFORMATION AND COMMUNICATION TECHNOLOGY RESOURCES

PROCEDURAL GUIDELINES

Definition:

The Board's network is defined as the set of communication facilities and devices operated and administered by the Huron-Superior Catholic District School Board to facilitate learning and communication.

These facilities and devices include, but are not limited to, electronic devices, routers, switches, Wi-Fi, telephones, mobile devices, electronic communication as well as third-party Internet services provided to the Board. Examples of third-party web services include and not limited to Office 365, Bright Space, as provided by the Ministry of Education, Google Workspace for Education and online classroom resources.. In addition, any electronic devices which access the board's network, ecosystem or infrastructure from within the board or access remotely will be deemed part of the network and subject to this procedure.

Acceptable use of Electronic Communication Tools:

Use of the Board's information and communication technology resources must be consistent with the Board's Mission Statement.

Activities inconsistent with the Board's Mission Statement are prohibited. These include:

- commercial use
- political lobbying/anti-board activities
- harassment or nuisance messages
- illegal activities are strictly prohibited and include, but are not limited to the following:
    - transmission of any material in violation of any law or regulation, such as copyrighted materials, threatening or obscene material, or material suggesting pornography, racism, sexism, or discrimination of any kind
    - use of the network to devise or execute any scheme to defraud
    - vandalism, such as any malicious attempt to damage or destroy equipment, software, data of another user, the Board's network, or any other device connected to the Board's network or email system
    - uploading, downloading, or creating computer viruses
    - attempting to access unauthorized resources, entities, or data

- activities that waste, degrade, or disrupt network resources or performance are prohibited
- unauthorized copying or installation of unlicensed software is not permitted. All software installed on Board-owned devices must be fully licensed and installed according to the software provider's licensing agreements.

Privacy, Security, Reliability and Ownership of Data:

Board technology resources, local data and cloud data through contractual agreements with third party vendors, including email, electronic files, and information in computer systems, is Board property and may be reviewed, monitored and accessed by authorized individuals, as needed. Data is also subject to relevant legislation and may be accessed through Freedom of Information requests.

Users of the board's resources should have no expectation of privacy with respect to any use of the Board's information resources. The board has the right, without consent from employees, students or other users, to monitor any and all aspects of its information resources including, without limitation, reviewing documents created and stored on its computer system; deleting any matter stored on its information resources; monitoring websites visited by users; monitoring chat, conferencing, and groups; reviewing all material downloaded or uploaded by users from the internet; and reviewing email sent and received by users. If policy violations are discovered, this will result in an investigation and necessary action will be taken, where appropriate.

Information stored on personally owned devices is the responsibility of the device owner/user. However, personally owned devices which are used for creating, displaying, storing or sending fraudulent, harassing, sexually explicit, profane, obscene, intimidating, defamatory or otherwise inappropriate or unlawful materials that impact school climate will result in a full investigation and necessary action will be taken, where appropriate.

The Board makes no warranties of any kind, whether expressed or implied, for the services it is providing. The Board will not be responsible for any damages suffered by the user. This includes, but is not limited to, loss of data resulting from delays, non-deliveries, miss-deliveries, or service interruptions caused by its own negligence or the user's errors or omissions. Use of any information obtained via the Board's network is at user's risk. The Board specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Network Etiquette:

Users are expected to abide by the generally accepted rules of network etiquette and responsible behavior related to the appropriate use of technology.

These include, but are not limited to, the following:

- Be polite and respectful in your electronic communications with others.
- Do not write or send annoying or abusive messages to others.
- Do not invade the privacy of others.
- Use appropriate language; do not swear or use vulgarities.
- Keep file transfers to a minimum, recognizing that computer resources are limited and valuable.
- Stay on topic and keep messages short and to the point.

User Responsibilities:

a) ALL USERS MUST:

- Ensure that technology is used in accordance with Board policies and procedures.
- Comply with the board and school's Code of Conduct.
- Ensure that technology is used to support teaching and learning in accordance with HSCDSB's teaching and learning expectations.
- Use technology in a lawful, responsible and ethical manner, consistent with the purposes for which it is provided.
- Ensure that their personal network login and password are secured, protected and not shared with anyone. Users will immediately notify the system administrator if their password is lost or stolen, or if they have reason to believe that someone has obtained unauthorized access to their account.
- Ensure that photos, videos or images of an individual/group are not posted online/shared digitally unless consent from the individual(s)—over the age of 18—or parental consent (for those under the age of 18) has been obtained.
- Ensure that technology is not used for political or union business unless approved by the board.
- Care for and maintain their personal devices and its security. The Board is not responsible for the replacement of lost, stolen or damaged items.
- Care for any equipment or devices owned by the board.
- Report lost, stolen, or damaged equipment to direct supervisors/teachers.

b) PRINCIPALS MUST:

- Ensure that staff are aware of the Board policy and procedures.
- Establish and monitor digital citizenship and responsibility through the board and school's Code of Conduct.
- Instruct and model, for staff and students, digital citizenship and responsibility.
- Authorize in the school the use of technology for the sole purpose of enhancing academic achievement, while respecting the dignity and safety of all members of the school community.
- Ensure that all students and parents are aware of the students' rights and responsibilities regarding the use of information technology, including protection of privacy and security of Board systems.
- Ensure that a record of signed Usage of the Boards Computers, Network, Internet and Email application and agreement is kept students at the school in the Student OSR and employees kept with the Human Resources Department
- Ensure that parental permission is obtained during the registration process for the publication of student pictures and information on publicly accessible sites Identification of students for school related activities.
- Facilitate technological accessibility for all students.
- Monitor student use of the network, board owned and personal devices for appropriate use, as well as establish school procedures for the use of technology in the school and classroom.
- Address abuse of technology resources in a manner consistent with the Board and school Code of Conduct
- Ensure that any information accessed or posted to school, student or public sites is consistent with the Municipal Freedom of Information and Protection of Privacy Act.

c) TEACHERS MUST:

- Supervise students' use of technology within the teacher's assigned teaching area.
- Instruct and model digital citizenship and responsibility for students.
- Determine when students are able to access Board technology or their personally owned devices for educational purposes only.
- Check with the Principal to ensure that there is parental consent before posting pictures and information for students on publicly accessible sites.
- Refer to the Ontario College of Teachers Professional Advisory: Maintaining Professionalism - Use of Electronic Communication and Social Media.

d) STUDENTS MUST:

- Students 18 years of age and over must review and sign-off the Usage of the Boards Computers, Network, Internet and Email application and agreement.
- Use Board technology for curriculum-related/educational purposes only.
- Demonstrate digital citizenship through the appropriate use of technology, as outlined in school's codes of conduct.
- Ensure the security of their personal technology. The board is not responsible for devices becoming lost, damaged or stolen.
- Respect the privacy of themselves and others by protecting all sensitive personal and confidential information contained on any digital device.
- Take pictures, recordings or live-stream of other students or staff under the direct supervision of a teacher and share them outside the classroom only with expressed teacher permission.
- Be responsible for online actions and behavior on or off school property during or outside of the school day, as they have an impact on the school climate.
- Report any inappropriate use of email, data or unauthorized technology to a teacher or administrator immediately.
- Understand that computer use is a privilege, not a right. Students are responsible for any equipment they are issued or use.
- Attend to the safety and security of any device issued to them (e.g., do not place laptops on the corner of a desk where they may be knocked over, do not use devices with food and drink nearby, do not deface any device by removing keys from keyboards).
- Report any damage that occurs to a device that is in their possession. See Missing/Damaged Digital Device Form.

e) PARENTS/GUARDIANS MUST:

- Complete the Board Student Application for Usage of the Boards Computers, Network, Internet and Email application and agreement for students under the age of 18
- Review any information provided by the school to the school community about the ethical use of the Internet and personal technology in our Catholic faith community.
- Agree to support a safe and respectful learning environment by:
    - Modeling respect, responsibility and civility online (digital citizenship).
    - Being an active, positive participant in the online community.
    - Encouraging respectful and appropriate online behavior.
- Respect the privacy of other students/parents/school staff before posting pictures/videos online of school-sponsored events.

Anti-Spam

Canada's Anti-Spam Legislation came into effect on July 1, 2014. Under the legislation, anyone (including teachers, principals, office staff, etc.) who send an electronic message that encourages participation in a commercial activity must do the following:

1. Obtain the consent of the recipient
2. Provide identification information about the sender
3. Provide an unsubscribe option so recipients can remove themselves from the list

What is a commercial electronic message?

A commercial electronic message is a message sent to an electronic address that encourages participation in a commercial activity. Examples of electronic messages include emails, text messages, instant messages, telephone messages or direct messages on social media (e.g. Facebook or Twitter).

Messages are considered commercial when they have to do with the purchase of a good or service. Examples of commercial electronic messages you might receive from your school include messages about:

- Fundraising events
- Yearbook sales
- Sale of student photos
- Information about purchasing team uniforms
- School newsletters that contain commercial information

For more information on CASL, visit the Government of Canada's website: www.fightspam.gc.ca

Password Policy for Staff:

The Huron-Superior Catholic District School Board will use an enforceable password policy to provide greater security. Forced password changes every 365 days with historical logging and complexity will be utilized to maintain a highly secure environment for all users. All employees must use Dual-Factor Authentication.

Enforcement of Terms and Conditions:

The use of the Board's network is a privilege, not a right. Penalties for violation of these terms and conditions may range from temporary to permanent withdrawal of privileges,progressive disciplinary action, suspension/expulsion, employee termination to prosecution under the law. Upon consultation with administration and the Information Technology Department, an account may be closed or suspended at any time.