



Policy: Responsible use of Technology

Policy Number: AH

Policy Type: Personnel

Policy

Hanover School Division supports the use of technology to enhance and facilitate learning. Technology encourages educational environments that are innovative, creative and engaging. This policy applies to student, visitor and staff use of HSD and personal technology.

1. Use of Personal Technology Devices for Staff, Students, and Visitors

Background and Definitions

Staff, students, and visitors are required to follow Manitoba Education’s Guidelines for Cellphone Use, HSD’s Responsible Use of Technology Policy, and any additional expectations set out by each individual school.

Personal Technology: refers to electronic devices and tools designed for individual use to assist with communication, entertainment, productivity, and daily activities..

Personal Cellphone: refers to a portable, wireless device owned and used by an individual for private communication and personal tasks.

Personal Communication Device: refers to a communication device as any tool, instrument, or technology that facilitates the transmission of information between individuals or groups. These devices can be electronic, digital, or analog and are used for various forms of communication, such as voice, text, video, or data exchange.

Staff Personal Cellphone and Communication Device Use:

- During contact time or in a position of supervising students, staff should not use their personal cellphone unless granted permission from the school principal.
- During preps and breaks, staff have permission to use their cellphone.
- Staff should not store any images, videos, or audio recordings of students, staff or school property on their personal cellphone.

Student Personal CellPhone and Communication Device Use:

In the Hanover School Division we aim to cultivate an optimal learning environment that minimizes distractions and promotes focused engagement in all school activities. By prohibiting the use of cellphones and communication devices during school hours for K-8 and limiting cellphones and communication devices for Grades 9-12, we seek to foster a culture of attentiveness, active participation, and respectful interaction among students and staff. This aligns with our commitment to prioritizing educational excellence and ensuring the well-being of our students.

Students are required to follow the expectations set out by Manitoba Education, School Division, and school.

Kindergarten to Grade 8 Students are not permitted to bring a cellphone or personal communication device to school. These grades are considered Cellphone Free.	Grade 9 to 12 Students in grades 9 to 12 are not permitted to use cellphones and communication devices during class time. Cellphones and communication devices should be stored in a designated area (e.g., backpacks, lockers, or
--	---

<ul style="list-style-type: none"> If a student requires the use of a personal device for notification to administer medication or additional health-related concerns, an accommodation can be provided by the school principal. 	<p>classroom storage) and kept on silent mode.</p> <ul style="list-style-type: none"> Exceptions are allowed for educational purposes when explicitly directed by the classroom teacher. In such cases, the teacher will provide clear instructions on when and how cellphones may be used.
<ul style="list-style-type: none"> Students are not permitted to bring their personal cellphone or communication device on field trips or for events that occur during the school day. 	<ul style="list-style-type: none"> With teacher permission, students can bring their cellphone on a field trip and extra-curricular activities. The teacher/coach is responsible for setting expectations.
	<ul style="list-style-type: none"> Students are not permitted to use their personal devices to take a picture, video, or voice record of another student or adult without their permission.
	<ul style="list-style-type: none"> The use of cellphones or cameras is strictly prohibited in all school washrooms and change rooms, including washrooms and change rooms on field trips.
	<ul style="list-style-type: none"> Use of personal technology devices with a digital camera <u>for any reason</u> during a test or assessment will result in the removal of the student from the assessment and the assessment will be considered invalid. A mark of zero may be assigned or an alternative assessment may be possible.
	<ul style="list-style-type: none"> Recordings made secretly and/or used maliciously will result in disciplinary action up to and including expulsion and a police report.

Policy Enforcement

Each school will set appropriate enforcement of the HSD Policy AH - Respectful Use of Technology.

- Any use of a cellphone or a communication device during prohibited times or in an inappropriate manner may result in immediate confiscation of the device by school staff. The device will be stored at the school office. Parents/caregivers can be requested by the school principal or designate to come to the school and pick up their child's cellphone or communication device.
- Further disciplinary action may result in but is not limited to the student not being able to bring their cellphone or communication device to school.

Visitors Cellphone Use

- All visitors to the school must sign in at the office.
- During the school day, visitors are not permitted to use the camera or voice recorder on school property, unless the school principal/designate has given permission.
- During extra-curricular activities hosted on HSD school property, visitors are permitted to use their cellphone. Visitors are discouraged from sharing or posting videos or pictures to social media without permission from the individuals in the picture or video.

Personal Device Damage

Hanover School Division assumes no responsibility for the loss, destruction, or theft of any personal technology device brought to school or to any school-related activity by a student staff, or visitor.

Sanctions

All forms of disciplinary action will be in accordance with Policy JFA Student Discipline.

2. Employee Responsible Use of Divisional Telecommunication and Network Services Agreement

Background

Hanover School Division offers employees, students, and other authorized users (as determined by the Information and Communication Technology Services (ICT Services) department and school and department administrators), access to a variety of information technology resources. These include but are not limited to computer workstations, cellphones, wired and wireless networks along with controlled access to the Internet.

All HSD buildings allow for wired and wireless network access to all resources hosted locally or in a cloud service such as, but not limited to, Google or Microsoft Azure.

In response to the privilege of accessing the Internet, every Internet user has the responsibility to respect and protect the rights of every other user on the Internet, and to act in a responsible, ethical, and legal manner.

Use of the wired or wireless networks within HSD along with using any Divisionally-owned devices is a privilege that may be revoked at any time for abusive conduct.

Wired and wireless networks are a shared resource, which is the property of the School Division and, as such, may be subject to Division-authorized search to ensure the integrity of the networks and compliance with policies and laws. If there is reason to believe that there has been misuse of Division resources, user accounts may be accessed by network administrators.

Responsible use of information technology includes, but is not limited to, the following:

- Use consistent with the mission of Hanover School Division,
- Use that encourages efficient, cooperative, and creative methods to perform the user's job duties or educational tasks
- Use related to instructional, administrative, and other support activities considered consistent with the mission of the Division
- Must follow FIPPA and PHIA regulations
- Posting student work to the Internet will require an HSD Permission to Publish form signed by parents/caregivers.

All teachers have a responsibility to work together to help students develop the skills needed to discriminate among information sources, to identify information appropriate to student age and development levels, and to evaluate and use the information to meet students' educational goals.

Employee Use Guidelines on Network and Divisional Email

The Internet allows people to access networks and computers, including local, national, and international resources such as libraries, government agencies, universities, K-12 schools, discussion groups, software, and technical information.

Email Expectations

All employees are encouraged to use email and telecommunications tools and apply them daily in appropriate ways to the performance of tasks associated with their positions and assignments.

Employees with email accounts will be responsible for checking, reading, and responding when necessary to email messages regularly during the school day.

Furthermore, HSD expects that all staff will use the email system in a responsible and ethical manner. All network and email users are expected to abide by the generally accepted rules of network etiquette.

The following actions will **not** be permitted on HSD network and Email:

- Using abusive language, including hate mail, harassment, or discriminatory remarks.
- Deliberately accessing inappropriate content that contain obscene material, including reviewing, downloading, storing, or printing files or messages that are obscene, vulgar, or sexually explicit, or that use language that degrades others.
- Employees are strictly prohibited from sharing their personal passwords associated with any HSD managed accounts under any circumstances.
- Using anything as public without the permission of the author(All communications and information accessible through the Internet or other computer networks should be assumed to be private property).
- Maliciously attempting to harm or destroy data of another user, school or Division networks, or the Internet, including uploading or creating viruses.
- Using networks for any illegal activity, including violation of copyright or other laws.
- Using networks for a commercial, political or profit-making enterprise, except as specifically agreed to with the Division.
- Using or accessing a file or an account owned by another user without his/her permission, or deliberately distributing or downloading any material in such a manner that causes congestion of networks.
- Installing software that is not legally licensed for use (i.e. pirated software).
- Installing software that is not supplied or approved for use by the Division without authorization by an administrator.
- Installing any hardware not owned by the Hanover School Division.
- Using Division resources to facilitate illegal duplication of copyrighted materials.
- Hosting or sharing any student information on non-sanctioned cloud storage systems.
- Send personal group messages to schools and/or the entire Division (such as to sell a personal possession, look for a roommate, etc.).
- Distribute chain letters or to participate in email games or other non-business related activities.

Downloading Files from the Internet

There is always a risk that downloaded software may pose a threat to Hanover School Division computer systems. If authorized users locate a file that they have a need to acquire, they are required to take the following precautions:

- Make sure the file is within the guidelines of Division policies and regulations on the responsible use of technology.
- Apply available approved virus scanning software on the file before the file is opened or launched.

Employee Supervision of Student Network Use

- While in the classroom environment, teachers are responsible for supervising their students while on the internet. If “free time” is provided to students while using the internet, students must be provided with the educational purpose for the use of the internet during their free time.

Security Training

- ICT Services will provide all staff with Online Security training over the course of the school year. All staff within HSD have the responsibility to protect and maintain the security of all staff and student data. Security Training is a key component in the protection and security of data.

Sanctions

In the event that an employee willfully violates any of the above policy as it pertains to the Use of HSD Information Technologies and Employee Responsibilities, may result in a loss of access privileges and, in turn, may necessitate disciplinary action. Any misuse or illegal activities will result in temporary or permanent cancellation of privileges, disciplinary action up to and including dismissal. If a violation of law has occurred, contact with law enforcement authorities will be made.

All staff will sign the Policy Compliance Certification document upon hire, which includes the Employee Responsible Use of Divisional Telecommunication and Network Services Agreement.

Use of Information Technologies & Student Responsibilities

Background

Hanover School Division offers employees, students and other authorized users (as determined by ICT Services, and school and department administrators) access to a variety of information technology resources, including computer workstations, local area networks, a wide area network, and the Internet.

Electronic research skills are fundamental to the preparation of citizens and future employees. HSD expects that staff will blend thoughtful use of such information throughout the curriculum and that staff will provide guidance and instruction to students in the appropriate use of such resources.

Students are responsible for appropriate behaviour on school computer networks just as they are in a classroom or a school hallway. Communication on the network is often public in nature. General school rules for behaviour and communications apply. The network is provided for students to enhance learning and communicate with others. Access to network services will be provided to students who agree to act in a considerate and responsible manner.

Supervision

Grades K-8: Students are supervised by a teacher while accessing the internet.

Grade 9-12: Students must adhere to HSD Respectful Use Policies (RUPA) while using digital devices, both personal and school-provided, on campus. Network privileges may be revoked if they violate HSD policies.

General Use Guidelines of HSD Network and Email

Students are responsible for appropriate behaviour on school computer networks just as they are in a classroom or a school hallway. Communications on the network are often public in nature. General school rules for behaviour and communications apply.

The network is provided for students to conduct research and communicate with others. Access to network services is given to students who agree to act in a considerate and responsible manner. Parent permission is required. Access is a privilege - not a right. Access entails responsibility.

Individual users of the Division computer networks are responsible for their behaviour and communications over those networks. It is expected that users will comply with Division standards and will honour the agreements they have signed. Beyond the clarification of such standards, the Division is not responsible for restricting, monitoring or controlling the communications of individuals utilizing the network.

Network storage areas should be treated like school lockers. Network administrators may review files and communications to maintain system integrity and ensure that users are using the system responsibly. Users should not expect that files stored on Division servers will remain private.

Within reason, freedom of speech and access to information will be honoured. During school, teachers of younger students will guide them toward appropriate materials. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, movies, radio, and other potentially offensive media.

HSD is committed to educating responsible digital citizens who RESPECT, EDUCATE, and PROTECT themselves and others.

Students who come across any information that is obscene, vulgar, sexually explicit, or offensive should immediately inform a teacher or other adult staff member.

When using HSD technology or personal devices, all students are required to:

- Take precautions to ensure personal privacy is protected (avoid sharing personal or identifying information online).
- Protect the privacy of others (do not share their personal information, images, or video without consent).

- Be respectful to all (do not use technology to degrade, defame, bully, or harass others).
- Avoid inappropriate or offensive online content (do not access, forward, or share).
- Abide by copyright laws and fair-use guidelines for electronic content.
- Do not post/download/share illegal software, music, movies, or content.
- Report any concerns, misuse, or abuse of technology to school personnel.
- Take full responsibility for, and respectfully use any technology provided.
- Use personal technology only when permission is granted, and keep it stored away when not in use.
- Turn off all peer-to-peer software when using personal technology at school (music, video, and file-sharing).
- Connect only to school approved Wi-Fi sources or networks.

When using email and other communication systems, students are expected to abide by school and Division policies and rules, and the generally accepted rules of network etiquette. These include, but are not limited to, the following:

- Refrain from any abusive language. Swearing, vulgarities, and other similar use of language is not acceptable and will not be tolerated.
- Do not give out any personal information such as a home address, telephone number, parent's or guardian's name, etc.
- Do not send fraudulent, intimidating, or anonymous messages.
- Do not participate in defamatory attacks on individuals or organizations.

Sanctions

- Violations of any of the outlined guidelines may result in a loss of access privileges and, in turn, may necessitate withdrawal from any technology-related courses in which a student may be enrolled.
- **Additional disciplinary action may be determined regarding inappropriate language or behaviour, up to and including suspension or expulsion.**
- Individual students and their parent(s)/legal guardian(s) may be held liable for violations of the outlined guidelines.
- When applicable, law enforcement agencies may also be involved.

Student Responsible Use Agreement & Parent Permission Form

Hanover School Division provides its students access to the Division computer network for Internet use as well as other online services. To gain access to the Internet, all students under the age of 18 must obtain parental permission and must sign and return this form to their school. Students 18 and over may sign their own forms.

Access to the Internet will enable students to explore thousands of libraries, databases, and bulletin boards while exchanging messages with Internet users throughout the world. Families should be aware that some materials accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people. While our intent is to make content-filtered Internet access available to further educational goals and objectives, students may find ways to access other materials as well. The benefits to students from access to the Internet, in the form of information resources and opportunities for collaboration, outweigh any disadvantages, but ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. Hanover School Division supports and respects each family's right to decide whether or not they approve of providing access to the internet for their child.

Date Policy Created	August 21, 2007
Date of last Review:	March 4, 2025
Reference(s):	Policy JFA - Student Discipline
Related Forms:	