



POLICY

Use of Personal Electronic Devices by Staff, Students or Visitors to the School

Staff and visitors to the school, in possession of a personal electronic communications device, must have it turned off at any time they are in class, supervising students in school or participating in any school event. Staff must not send or receive personal communications while on duty.

Use of communication devices for emergency communications related to safety and well-being of students, staff or visitors is allowed, at the discretion of the administrator.

Individual schools are authorized to set general limitations on possession of electronic devices of any kind, including cell phones, digital cameras, music or video players and gaming devices.

Students with administrative permission to be in possession of electronic devices in school are bound by the following conditions:

All communication devices must be turned off when the student boards the school bus or enters the school building. These devices may not be activated when classes are in progress or during any school event during the regular school day. Students may not leave class to make or receive an electronic communication - cell phone call, text message or internet communication.

During school outings, field trips or extracurricular events, use of a cell phone is by permission of the supervising academic staff (principal or teacher) or the designated community coach, where no academic staff is present.

Use of electronic communication devices or digital cameras for any reason during a test or assessment will result in removal of the student from the assessment and the assessment will be considered invalid. A mark of zero may be assigned.

Cell phones equipped with cameras should be avoided. Cameras or phones equipped with cameras must be kept out of sight and not activated in washrooms, change rooms or any other private areas. Use of an electronic communications device or digital camera to record video, still shots or sound must be done with express permission of the supervising staff member and with full advance knowledge and permission of any individual or group being recorded. Sharing, distribution or broadcasting of any such material must be done with full permission of every individual being recorded. Posting to the Internet may require written permission of parents. Recordings made secretly and/or used maliciously will result in disciplinary action up to and including expulsion and a police report.

Any use of an electronic communication device during prohibited times or in an inappropriate manner will result in immediate confiscation of the device by school staff. Devices will be returned to parents or guardians under conditions set by administration.

Hanover School Division assumes no responsibility, in any cases, for the loss, destruction or theft of any electronic device brought to school or to any school related activity by a student.

USE OF HSD INFORMATION TECHNOLOGIES & EMPLOYEE RESPONSIBILITIES

Hanover School Division offers employees, students and other authorized users (as determined by the computer department, 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.



Local or Wide Area Network (LAN or WAN) -- Each Division school and building has access to a local area network or wide area network (computer network) that allows data connectivity among classrooms, media centers and offices.

In response for 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 Internet, Division computer networks and computer workstations is a privilege, which may be revoked at any time for abusive conduct.

Any misuse or illegal activities will result in any or all of the following:

- temporary or permanent cancellation of privileges
- **disciplinary action up to and including dismissal**
- contact with law enforcement authorities, if a violation of law has occurred

The networks (LAN and WAN) are a shared resource, which are 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.

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

- Use consistent with the mission of the 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

All educators 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 information to meet students' educational goals.

GUIDELINES

Employee Use Guidelines

The Internet, an international network of networks, 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, technical information, news and weather.

The Internet, district computer networks and computer workstations must be used responsibly, ethically and legally. Failure to adhere to Division policies, regulations and guidelines for the use of computers, networks and the Internet will result in a revocation of access privileges.

The following actions will **not** be permitted:

- Using abusive language, including hate mail, harassment or discriminatory remarks
- Deliberately accessing inappropriate websites 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



- 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 Hanover School Division
- Using Division resources to facilitate illegal duplication of copyrighted materials.

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 acceptable 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

Hanover School Division employees are responsible for supervising student use of the Internet. All school student use of the Internet is to be supervised.

Students will be asked to turn in a signed copy of the *"Internet Acceptable Use Agreement and Parent Permission Form"* before being granted access to Internet resources.

Network and E-mail Etiquette

Regulations covering acceptable use of the email system are covered in a separate policy. Refer to the document entitled: *"Employee Guidelines for Acceptable Use of Divisional Email Services"*.

Network storage areas are Divisional property. Network administrators may review files and communications to maintain system integrity and insure that users are using the system responsibly. Users should not expect that files stored on Division servers are private.

SANCTIONS

Violations of any of the outlined guidelines by staff members 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.

Employee Guidelines for Acceptable Use of Divisional Email Services

With the spread of telecommunications throughout the modern work place, the Board recognizes that employees will shift the ways they share ideas, transmit information, and contact others. As staff members are connected to the global community, their use of new tools and systems brings new responsibilities as well as opportunities.



The Board encourages staff to make use of telecommunications to explore educational topics, conduct research, and contact others in the educational world. The Board anticipates that the new systems will expedite the sharing of effective practices and lessons across the Division and will help staff stay on the leading edge of practice by forming partnerships with others across the nation and around the world.

All employees are encouraged to use electronic mail 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 year.

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

As such, employees are **NOT** permitted to use the email system:

- to send unsolicited email messages to groups and/or the entire Division announcing non work-related events or activities.
- to send personal group messages to schools and/or the entire Division (such as to sell a personal possession, look for a roommate, etc.)
- to distribute chain letters or to participate in email games or other non-business related activities
- to participate in defamatory or other unprofessional attacks on individuals or organizations
- to access another user's email account
- for commercial, profit-making or political campaign purposes.
- to send fraudulent, intimidating or anonymous messages.
- to share confidential information about students or other employees as email messages are not entirely secure.
- to send or display offensive messages or pictures.
- to distribute files that may introduce a virus to the system. All email enclosures are to be verified as virus-free before distribution. As a further precaution, all incoming email enclosures should also be verified as virus-free. The integrity of any files introduced to the system is the sole responsibility of the user.
- to illegally distribute copyrighted material
- to distribute any material in such a manner that causes congestion of networks. (i.e. distribution of excessively large enclosures)

In order to ensure the reliability and integrity of the email system, employees are to be aware of the following:

- Communication over networks should not be considered private. Network supervision and maintenance may require review and inspection of directories or messages. Messages may sometimes be diverted accidentally to a destination other than the one intended. Privacy in these communications is not guaranteed.
- The Division reserves the right to access stored records in cases where there is reasonable cause to expect wrong-doing or misuse of the system. Network administrators may review files and communications to maintain system integrity and to ensure that staff members are using the system responsibly. Users should not expect that files stored on Division servers will be private.
- As communications over the network are often public in nature, general rules and standards for professional behavior and communications will apply.



In the event that an employee willfully disregards the acceptable standards for use of the email system as outlined above, the Computer Department will report violations to the employee's supervisor who will take appropriate action. **Violations may result in a loss of access and/or disciplinary action up to and including dismissal.** When applicable, law enforcement agencies may be involved.

I have read and understand the conditions for employee use of technology and the HSD computer/Internet system. I hereby agree to comply with the above stated rules pertaining to the acceptable use of technology in the division.

Employee Signature _____ Date: _____

Use of Information Technologies & Student Responsibilities

Hanover School Division offers employees, students and other authorized users (as determined by the computer department, 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 information research skills are fundamental to preparation of citizens and future employees during an Age of Information. The Board expects that staff will blend thoughtful use of such information throughout the curriculum and that the staff will provide guidance and instruction to students in the appropriate use of such resources.

Students are responsible for good behavior 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 behavior and communications apply. The network is provided for students to conduct research and communicate with others. Access to network services will be provided to students who agree to act in a considerate and responsible manner.

Use of the Internet and other computer networks will take place in teacher supervised settings. Before a student is permitted to access the Internet, the student and his or her parent or guardian will be asked to complete and return the form entitled "*Internet Acceptable Use Agreement & Parent Permission Form*".

General Use Guidelines

- Use of the Internet, other computer networks and computer workstations is a privilege, which may be revoked at any time for abusive conduct.
- Access to the Internet will be for educational purposes.
- In addition to the Division's standard consequences for student misbehavior, any network misuse or illegal activities will result in temporary or permanent cancellation of network privileges, contact with the student's parent(s) or guardian(s) and, if a violation of law has occurred, contact with law enforcement authorities.

The following actions will **not** be permitted:

- Using abusive language, including hate mail, harassment or discriminatory remarks;
- Accessing inappropriate websites that contain objectionable, offensive or obscene material, including reviewing, downloading, storing or printing files or messages that are obscene, vulgar, sexually explicit or that use language that offends or tends to degrade others;

- 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.);
- Deliberately attempting to harm or destroy data of another user, school or Division network, or the Internet, including uploading or creating viruses;

Using networks and /or Division resources for any illegal activity, including violation of copyright or other laws;

- Using networks for a commercial, political or profit-making enterprise
- Gaining unauthorized access to resources or entities;
- Using an account owned by another user, with or without their permission;
- Deliberately distributing any material in such a manner that might cause congestion of networks.
- Downloading and/or installing unauthorized software or hardware on school systems

Students who come across any information that is obscene, vulgar, sexually explicit or offensive should immediately inform a teacher or other adult staff member. Students are responsible for not pursuing this type of information.

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 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.

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

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 at the building level in line with existing practice 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 Acceptable Internet Use Agreement & Parent Permission Form

Hanover School Division is pleased to provide its students access to the Division computer network for Internet use as well as other on-line 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 warned 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. We believe that the benefits to students from access to the Internet, in the form of information resources and opportunities for collaboration, exceed 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. To that end, the Hanover School Division supports and respects each family's right to decide whether or not to apply for access.

Division Internet Rules

Students are responsible for good behavior 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 behavior 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 behavior and communications over those networks. It is expected that users will comply with Division standards and will honor 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 may 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 honored. 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.

As outlined in Board policy and procedures on student rights and responsibilities, students are not permitted to:

- Send, display or download offensive messages or pictures
- Release personal information such as their address, phone number, parent or guardian's name, etc...
- Use obscene language
- Harass, insult or attack others
- Willfully damage computers, computer systems or computer networks. Such instances include, but are not limited to:
 - Propagation of computer worms or viruses
 - Denial of service attacks
 - Using the network to gain unauthorized access to any computer on the network



- Violate copyright laws
- Use another's password
- Trespass in another's folders, work or files
- Intentionally waste limited network resources by downloading movie, music, games, or programs.
- Employ the network for commercial purposes
- Download and/or install unauthorized software or hardware on workstations

Violations may result in a loss of access as well as other disciplinary or legal action.

As a user of the Hanover School Division computer network, I hereby agree to comply with the above stated rules; communicating over the network in a reliable fashion while honoring all relevant laws and restrictions.

Student Signature _____ Date: _____

As the parent or legal guardian of the minor student signing above, I grant permission for my son or daughter to access networked computer services such as the Internet. I understand that individuals and parent(s)/legal guardian(s) may be held liable for violations. I understand that some materials on the Internet may be objectionable, but I accept responsibility for guidance of Internet use, and setting and conveying standards for my daughter or son to follow when selecting, sharing or exploring information and media.

Parent Signature _____ Date: _____

Guidelines for School Websites

Given that the Internet is quickly becoming the medium of choice for disseminating information, the Board realizes the potential school websites hold as a public relations tool for keeping communities informed of events and activities at schools and to improve enrollment.

The Board, therefore, expects that each school in the Division will maintain a presence on the World Wide Web through a school website. In addition, the Board reasonably expects that the school will make every effort to ensure that the content presented on the web site changes regularly and, more importantly, is kept current.

School Website Content

School websites **may** contain the following information:

- School Contact Information
- School Address
- Phone Number
- Fax Number
- Email Address
- School Hours
- School Staff Listing
- School Profile
- Monthly Newsletter

School websites should **not** contain:

- Advertising or commercial logos or endorsement of commercial products, companies or organizations with the exception of school programs run in partnership with outside organizations.
- School maps or classroom locations

When creating web pages for the site, schools should be sensitive to copyright issues when using clip art images and background textures as accents for the website.

Posting Photographs on School Websites

- Group or action pictures of students and classrooms may be posted, providing individual names do not accompany the picture.
- Individual head and shoulder photos of students are generally to be avoided and may only be used with a signed permission form. First name only should be used. Refer to the form entitled "*Parent Permission Form for Web Publishing of Student Photograph*".
- Individual staff pictures may be used only with the prior consent of the staff member.

Posting Student Work on School Websites

- Permission is required from both the student and the parent before posting student work on school websites. Refer to the form entitled "*Parent Permission Form for World Wide Web Publishing of Student Work*".
- Student work should appear with a copyright notice prohibiting the copying of such work without express written permission.
- In the event that permission is requested to copy a student's work, such requests will be forwarded to the parent or guardian.
- Student work is to be identified only by a student's first name.

Identifying Recipients of School Awards or Special Honors

- In instances where list of students (i.e. award winners) are published in local newspapers or in the school newsletter, the information is in the public domain and schools may therefore identify such award winners by first and last name on their websites, providing pictures do not accompany the list.



**Parent Permission Form
for World Wide Web
Publishing of Student Photographs**

Name of Student: _____

Name of Parent: _____

Name of School: _____

We understand that a photograph of our daughter or son is under consideration for publication on a web site associated with his/her school. A copy of the photograph is provided with this form for our review. No home address or telephone number will appear with such work and the work will be identified only by our son/daughter's first name.

Intended Use: (State how or where the photograph will be used) _____

Website Address where photo will appear:

http:// _____

I hereby consent, without further consideration, that the attached photograph may be posted to the website associated with the named school and used in a manner related to the intended use as stated.

Parent Signature: _____ Date: _____



**PARENT PERMISSION FORM
for World Wide Web
Publishing of Student Work**

Name of Student: _____

Name of Parent: _____

Name of School: _____

We understand that our daughter's or son's artwork or writing is under consideration for publication on a web site associated with the aforementioned school. We further understand that the work will appear with a copyright notice prohibiting the copying of such work without express written permission. In the event anyone requests such permission, those requests will be forwarded to us as parents or legal guardians. No home address or telephone number will appear with such work, and the work will be identified only by our son/daughter's first name.

Description of original work to be posted:

Website Address where work will be posted:

http:// _____

We grant permission for the web publishing as described above until the end of the current school year.

Parent Signature: _____ Date: _____

I, the student, also give permission for such publishing.

Student Signature: _____ Date: _____

Legal References:

Additional Information: Formally Policy D38

Appendixes: