Hanover Public Schools
Digital Technology Acceptable Use Policy

The Hanover Public Schools encourages the use of digital technology for completing educational assignments and professional responsibilities. The primary purpose of providing digital technology within the district is to support the educational goals and objectives of Hanover Public Schools. It is expected that all digital technology users will respect the rights of others, and will act in a way that reflects proper ethical and legal standards at all times.

The following Digital Technology Acceptable Use Policy applies to all faculty, staff, students, community members, and guests who use the district's digital technology or who access our network. Any violation of the terms spelled out below may result in loss of access to district digital technology and/or disciplinary/legal action.

1. Definition and Purpose

1.1. Hanover Public Schools provides access to its data network and Internet portal (the "network") for employees, students and authorized guests. This network includes all hardware used to deliver and receive data, as well as all software instrumental in viewing and working with data over the network. Any computer—whether purchased by the district or owned by an individual—that is connected to our network at anytime is considered part of the network and, thus, is subject to the terms of this DTAUP.

1.1.1. The network has been developed for educational purposes. It is intended to assist students and teachers by providing access to a wide range of information resources. The network also allows for efficient communication within the district, with parents, social service agencies, government agencies, businesses, et cetera.

1.1.2. Incidental personal use of digital technology and the network may be permitted as long as it does not interfere with the educational mission of the Hanover Public Schools.

1.2. "User" refers to any staff member, administrator, student, community member, or authorized guest who connects to the Hanover Public Schools' network, who uses digital technology belonging to the Hanover Public Schools or who accesses our network.

1.3. "Digital technology" is any device that creates, transmits, or accesses digital information, whether connected to the network or used in a stand-alone situation. "Digital information" or "digital media" is any data that is created, transmitted, or accessed by digital technology.

1.4. "Educational" refers to the process of teaching and learning that is tied to the curricula of the Hanover Public Schools and the Department of Education's Curriculum Frameworks.

2. Staff and User Responsibilities

2.1. The Director of Technology will oversee access to the network and will establish processes for authorizing software installation, for the archiving of e-mail and databases, for maintaining virus and spam protection, and for complying with the Children's Internet Protection Act (C.I.P.A.)

2.2. The building principal will maintain signed user agreements for students and staff; he or she is responsible for enforcing the DTAUP on-site.

2.3. When using the Internet for class activities, teachers will preview and select materials appropriate to the students and relevant to the course objectives. Teachers will help students develop critical thinking skills (i.e. assessing the reliability of information found on the Internet) and provide guidelines and resources to assist their students in focused research activities. While their students are on-line and under their supervision, staff must be actively vigilant of websites visited by students.

2.4. Any user who finds objectionable material on any digital device should inform an administrator immediately. This includes material that any user might locate by connecting to a website—whether intentionally or accidentally—or might find residing on a computer or the network.

2.5. No staff member may access the on-line grades or personal information of any student except for those students with whom he or she has a direct professional relationship at that time.

2.6. No staff member may access the on-line personal or professional information of another staff member (may they access it with the staff person's consent?) except when the employee's direct supervisor accesses the information, or directs another member to access the information, in the process of fulfilling his or her professional responsibilities.

2.7. Accessing or attempting to access another user's account without permission is strictly prohibited. Users may not intentionally seek information on, obtain copies of, or modify files, data, or passwords belonging to other users on the network.

2.8. All passwords or other means of accessing computers, servers, software, or the network within the Hanover Public Schools is the property of the school district. Any misuse, dissemination, or destruction of these passwords is vandalism, and may be punished through internal disciplinary means and/or through the courts.

2.9. Any person who accesses the district from outside the network does so with the same restrictions and responsibilities as outlined in this document.

2.10. Any person who illegally accesses the Hanover Public Schools' network with intent to damage the network may be subject to criminal and/or civil prosecution as well as internal disciplinary action.

2.11. Any Hanover student, faculty member, administrator, or staff member who libels or slanders any other Hanover student, faculty member, administrator, or staff member using digital technology may be subject to internal discipline and/or punishment within the courts.

3. District Limitation of Liability

3.1. Hanover Public Schools makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through its network will be error-free or without defect.

3.2. The district will not be responsible for any damages users may suffer, including but not limited to, loss of data or interruptions of service, or personal physical, psychological, or monetary damages.

3.3. The district is not responsible for the accuracy or quality of the information obtained through or stored on the network.

3.4. The district will not be responsible for unauthorized financial obligations arising through the use of the network.

4. Due Process

4.1. While on the network, the user agrees to take full responsibility for his or her actions. The Hanover Public Schools will not be held liable for the actions of anyone connecting to the Internet through this network. Therefore, all users shall assume full liability—legal, financial, or otherwise—for their use of the network.

4.2. Violations of the DTAUP can carry serious consequences and could result in the immediate suspension of the user's privileges. The administration and/or town, county, state, or federal authorities may take further disciplinary action. Disciplinary actions will be tailored to meet specific concerns related to the violation. These disciplinary actions may include termination of employment or student suspension or expulsion.

4.3. Any questions, suspicions, or allegations concerning adherence to the Digital Technology Acceptable Use Policy should be brought to the attention of the Director of Technology, building principal, or the Superintendent of Schools.

5. Search and Seizure

5.1. The network and all devices (except those purchased personally by the user) attached to it are the property of the Hanover Public Schools; the storage systems of these devices are therefore subject to inspection by the administration at any time. District-owned computers, whether attached to the network or not, are subject to inspection by the administration at any time. System users should expect limited privacy regarding the contents of their files stored on the network.

5.2. An individual search will be conducted if there is suspicion that a user has violated the DTAUP or the law. The nature of the investigation will be in relation to the context of the nature of the alleged violation.

6. Acceptable Use of Hanover's Digital Technology

6.1. All students, faculty, and staff are encouraged to explore any and all digital technology offered by the Hanover Public Schools, whether through installed hardware and software or through approved network connections.

6.2. All students, faculty, and staff are encouraged to share the digital media that they create (along with production techniques) with all other members of the Hanover community. Please, contact the Director of Technology for methods of dissemination.

6.3. In the "Web 2.0" world, social networking—the sharing of ideas, opinions, and media across networks (especially the Internet)—brings us all closer. Anyone who discovers interesting websites of educational value is encouraged to contact his or her teacher, school principal, or the Director of Technology for posting these sites in the appropriate places.

7. Unacceptable Use of Digital Technology

7.1. No member of the faculty, the staff, or the student body will use Hanover Public Schools' digital technology to defame, slander, or libel any person.

7.2. Cyber bullying, which is the repeated use by one or more students of an electronic expression (including the transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system, including but not limited to, electronic mail, internet communications, instant messages or facsimile communications, creation of web pages or blogs in which the creator assumes the identity of another person, the knowing impersonation of another person as the author of posted content or messages, or the distribution of communications to more than one person or the posting of material on an electronic medium that may be accessed by one or more persons), alone or in combination with any written or verbal expressions or physical acts or gestures, directed at a victim that: (i) causes physical or emotional harm to the victim or damage to the victim's property; (ii) places the victim in reasonable fear of harm to himself or of damage to his property; (iii) creates a hostile environment at school for the victim; (iv) infringes on the rights of the victim at school; or (v) materially and substantially disrupts the education process or the orderly operation of the school. See Massachusetts General Laws, Chapter 71. Section 370.

7.3. He or she will not engage in any illegal activities or use the technology for purposes other than as intended in an educational setting.

7.4. When faculty, staff, students, or guests of the Hanover Public Schools use the network they become an extension of the Hanover Public Schools and are expected to follow the guidelines of this policy. Inappropriate use will not be allowed.

7.5. The user will not:

- use obscene, mean-spirited, pornographic, profane, inflammatory, racist, threatening, or disrespectful language;
- engage in prejudicial or discriminatory attacks, sexual harassment, or other forms of on-line bullying;
- post false or defamatory information about a person or organization, or post information that could cause damage, panic, or disruption. This includes, but is not limited to, the posting of broadcast messages or any other actions that cause congestion of the network or interfere with the work of others;
- install unauthorized software or download unauthorized software from a remote location or copy software that belongs to the Hanover Public Schools without expressed permission of the Director of Technology;
- attempt to go beyond his or her authorized access (hack), make deliberate attempts to disrupt system performance, destroy data (by spreading computer viruses or by any other means), or engage in other illegal activities;
- access blocked or prohibited websites through proxy servers that remove identifying information about the user for the purpose of anonymity;
- access non-educational gaming sites;
- disseminate passwords, codes, access telephone numbers, or account numbers to unauthorized persons;
- change the configuration of a computer or network without administrative permission;
- use the network to access material that is profane or pornographic or that advocates illegal acts, violence, or discrimination towards other people (e.g., hate literature);
- use the network for lobbying or advertising or for passing on information of a purely personal interest;

- damage or vandalize computers, computer systems, or networks either through physical alteration or through the introduction of malicious digital agents, such as viruses;
- trespass in other's folders, work, or files, or use another's password.

8. E-mail

8.1. All e-mail created or received by an employee of a governmental unit is a public record. According to Massachusetts General Laws:

> "public records" shall mean all…documentary materials or data, regardless of physical form or characteristics, made or received by any officer or employee of any agency…to serve a public purpose (G.L. c. 4, § 7, cl. 26).

8.1.1. E-mail is, therefore, a public record and it is subject to the requirements of the Public Records Law, G.L. c. 66. Any member of the public may request copies of e-mail. Please note that even deleted messages are subject to disclosure because they are required to be backed up in our archives.

8.1.2. Users should consider e-mail messages to be equivalent to letters sent on official letterhead and therefore should be written in a professional and courteous tone. As the AUP of the Springside School in Pennsylvania states, "tone is difficult to discern in electronic communication. Electronic communication is best used as a medium for disseminating factual information and should not be regarded as a replacement for face-to-face communication."

8.2. Faculty, staff, or students must not subscribe to mass electronic mailings (e.g., chain letters, "jokes of the day," "horoscopes," "trivia," et cetera). Mass mailings take up valuable network space that should be used for educational purposes. If a faculty member joins a professional (educational) listserv, it is requested that he or she subscribe in digest format. Please, contact the listserv administrator or the Director of Technology for instructions on how to accomplish this.

8.3. The Director of Technology or the Systems Engineer monitors the network to ensure proper network operations. Principals, department heads, or supervisors may request detailed reports indicating e-mail and Internet usage.

8.4. Students are not allowed to access non-school e-mail accounts, including chat and instant messaging. In the event that students are given e-mail accounts through the Hanover Public Schools, all e-mail rules stated in this DTAUP apply.

8.5. Email accounts issued by Hanover Public Schools may not be used to bully, harass, or threaten any individual or organization; accounts will not be used to send chain letters, viruses, or hoaxes to other students, faculty, or individuals;

8.6. Student email accounts are filtered for language and content; any email that contains inappropriate language or content will not be delivered and appropriate disciplinary action will be taken. Disciplinary actions will be tailored to meet specific concerns related to the violation.

9. Web Publishing

9.1. The Hanover Public Schools websites are designed to provide a portal to enable communication among teachers, students, staff, administration, and the community. Material posted on the district's websites or web portal must reflect the high educational standards of the Hanover Public Schools.

9.2. To help to protect the safety of our students and the accuracy and security of district information, the guidelines and procedures listed below must be followed:

9.2.1. No student's personal information such as home address or telephone number may be posted on the Hanover Public Schools' websites. Students must have signed permission from their parent/guardian granting permission to post the student's work and or picture. The use of a student's name, picture, or demographic information on the website of an employee of Hanover Public Schools is prohibited, except with the permission of the Superintendent of Schools and the parent/guardian of the student.

9.2.2. Material posted on district websites must have prior approval of the principal. All links from a school's website to sites outside of the Hanover Public Schools network must be approved by the principal or his/her designee. At all times, there must be a good faith effort to verify the authenticity of material posted on the district's websites.

9.2.3. Photographs and images must be used in accordance with district policy.

9.2.4. Logos or trademarks used must have written permission from the person or organization that owns the logo or trademark. The Hanover Public Schools' name or copyrighted logos must not be used on a personal web page without permission of the Superintendent.

9.2.5. The creator of any district web page is responsible for ensuring that the information contained therein is of the highest editorial standards (spelling, punctuation, grammar, style, et cetera). The information should be factually accurate and current. If errors are observed, the Director of Technology, principal or designated school webmaster should be contacted to make the necessary corrections.

9.3. All teacher and staff professional websites must reflect the high educational standards of the Hanover Public Schools. There may be no links from a teacher's or staff member's professional website to his or her personal website or to other websites of a non-educational nature except with permission from the building principal, the Director of Technology, or the Superintendent of Schools.

10. Personal Computers

10.1. Faculty, staff, and student personal computers may be configured for Hanover Public Schools' network with approval from the Director of Technology.

10.2. Personal computers are not the property of Hanover Public Schools and will not be serviced by the Technology Department.

10.3. Personal computers must have up-to-date virus protection software in order to be placed on the district's network.

11. Copyright Infringement

11.1. Existing copyright law will govern the use of material accessed through the network. The user—any student, faculty member, administrator, staff member, or guest—will not infringe upon the copyright of works found on the Internet or within the network.

11.2. As has been stated earlier, all copyrighted material used on any of the district's web pages must have the expressed written permission of the person or organization that owns the copyright.