Hamilton Central School

Instructional Technology Responsible Use and Internet Safety Policy

Network Acceptable Use

Hamilton Central School District students, employees and non-employee “Agency” staff (i.e. BOCES employees) may be granted access to a very powerful computer network that not only connects them with information and other users in the District, but also allows users to contact computer systems across the country and around the world via the Internet. These students, employees and non-employee staff are hereafter commonly referred to as “users”, “students”, and/or “staff”, or some combination thereof.

Network accounts will be created for students and staff to permit access to applications, data, file storage, Internet, and print services from various computers throughout the District. Account names and passwords are unique and no one else should ever know them. Each individual is responsible for the security of his/her own account. This information should not be given to anyone for any reason. This includes, but is not limited to, sharing passwords with student teachers or substitutes, and leaving passwords in plain view for others to see. Further, users should not leave a computer unsupervised on which they are logged in, thus allowing other users to gain access. Any user who intentionally compromises or uses confidential account information will be subject to disciplinary actions, including loss of network privileges. In addition, all computers and devices in the District shall be only be accessed through the network, and not as individual workstations.

Users of the District’s computer network are responsible for their own behavior and will comply with all appropriate standards of conduct. Use of the school’s computer resources is subject to certain rules and responsibilities. Specifically, users may not:

- Download, install or run any software on school computers or network servers not specifically authorized by the Hamilton Instructional Technology Department and legally licensed by the district.
- Copy or remove software from school computers or network servers.
- Store personal data files on local hard drives. All data files should otherwise be stored in users’ network home directories, in Google Drive or on other or on other removable media (where available). Note, that home directory space is limited and users may store only data essential to school activities. Staff is responsible for maintaining their own home directory space. All server data is backed up nightly; storage on staff workstations (desktop) and/or removable media is at user’s own risk.
- Use school computers to distribute, download, run or reproduce illegal duplicates of copyrighted program or data files.
- Connect any personal device to any school computer or network connection, with the exception of the Staff-BYOD and Student-BYOD wireless networks.
• Attempt to repair, alter the operation of, intentionally damage or remove from the premises school computer hardware (including desktop computers, CPUs, displays, printers or any other peripheral equipment) or software. Please note: Removal of computer from District premises excludes District staff-assigned laptops and/or other devices such as iPads or Chromebooks.

• Use school computers to generate and/or distribute, in either printed or electronic form, profane, harassing or discriminatory messages or images.

• Attempt to discover, alter, or distribute personal network account information or engage in any other activity that may result in the loss of data or access to network services.

• Access another student’s or staff person’s network account to view, modify, copy, delete or distribute private files. This includes logging in with another user’s account credentials, and using a computer where another user is already logged in.

• Use the network in such a way that would disrupt the use of the network by others or cause data to be lost or corrupted.

• Attempt to reverse engineer or hack any files associated with security software installed on school computers or servers with the intent to defeat or alter its operation.

• Intentionally infect any school computer or server with a virus, Trojan horse, worm, etc…, knowingly propagate any malicious program through the network or used computers or servers to launch or participate in attacks on any other computers inside or outside our network.

• Use school computers to gain unauthorized access to computers, data, networks or other resources outside the District.

• Teachers who are issued laptop computers may not allow anyone to log into those laptops and may only permit a student to use the laptop when being directly supervised by the teacher for the purpose of classroom work (i.e. presentations). In this case, the teacher will access the student’s network account or removable media to open the desired file for the student to use. The student will remain supervised at all times.

The District reserves the right to limit and/or terminate network access privileges in the event it determines that an individual has violated any policy or regulation of the District or of any state or federal law, or that such person has otherwise utilized the District’s network in an inappropriate or irresponsible manner.

The District reserves the right to access all files and monitor all uses of the District’s computer technology equipment at its own discretion so as to establish and maintain an assurance that such equipment is not being used inappropriately. Subject to the restrictions of applicable law, the District reserves the right to disclose email and other content from a computer that utilizes the District’s computer network. Thus, users of the District’s computer equipment shall have no expectation of privacy with respect to such use.

All programs and data created and/or stored on District-owned computers and networks are considered to be the property of the Hamilton Central School District. All communications and information accessible via the network, therefore, should be assumed to be its private property.
Internet Acceptable Use

Rationale

Internet access is available to students and teachers in the Hamilton Central School District. We are very pleased to bring such access to our schools and believe the Internet offers vast, diverse, and unique resources to the educational community. Our primary goal in providing this service to teachers and students is to promote educational excellence in schools by facilitating research, resource sharing, innovation and communication. The Internet is an electronic highway connecting millions of computers all over the world and tens of millions of individual subscribers. Access to the Internet adds a significant dimension to the educational process by enabling users to share information, conduct research, communicate and collaborate with other computer users.

Students and staff will have access to:

- Electronic mail (e-mail) communication with people all over the world.
- Information and news from government agencies such as NASA as well as the opportunity to correspond with other research institutions.
- Vast online document archives.
- Digitized museum collections of art and other cultural and historical artifacts.
- Discussion groups on a plethora of topics ranging from Chinese culture to the environment to music and politics.
- Two-way, real-time video-conferencing.

With access to computers and people all over the world also comes the availability of material that may not be considered to be of educational value in the context of the school setting. Hamilton Central School District will take precautions to restrict access to controversial materials. However, on a global network it is impossible to control all materials and a persistent and resourceful user may discover controversial or objectionable information. We (the Hamilton Central School District) firmly believe that the valuable information and interaction available on this worldwide network far outweigh the possibility that users may procure material that is not consistent with the educational goals and philosophies of the District.

Internet access is coordinated through a complex association of government agencies, commercial providers, and international, regional and local networks. In addition, the smooth operation of the network relies upon the proper conduct of the end users who must adhere to the strict guidelines. Standards and instruction in proper use will be provided so that users are aware of their responsibilities. In general, responsible use requires efficient, ethical, and legal utilization of the network resources. Although computer areas will be supervised and user activities monitored, users will be expected to display high levels of personal integrity and
trustworthiness. If a Hamilton Central School District user violates any of these provisions, his or her account may be terminated and future access could possibly be denied.

Internet Acceptable Use

1. **Acceptable Use.** The purpose of NSFNET, which formed the original backbone network of the Internet, was to support research and education in and among academic institutions in the U.S. by providing access to unique resources and the opportunity for collaborative work. Student use of the Internet should be limited to educational purposes that are directly related to the curriculum the student is studying. Employee uses of the Internet should be limited to those that are directly related to the individual’s duties and responsibilities of employment. However, the limited, occasional or incidental use of the Internet by employees for personal, non-business purposes is acceptable to the extent that there is neither tangible cost to the District nor any negative impact on the District’s computer or network resources.

Use of another organization’s network or computing resources must comply with the rules appropriate for that network. Transmission of any material in violation of any U.S. or state regulation is prohibited. This includes, but is not limited to copyrighted material, threatening or obscene material or material protected by trade secret. Use for commercial activities is generally not acceptable. Use for product advertisement or political lobbying is also prohibited.

The State of New York has in effect a criminal statute which makes it a Class A misdemeanor punishable by up to a year in jail for a person “with intent to harass, annoy, threaten or alarm another person, to communicate or cause to be initiated by mechanical or electronic means or otherwise, with a person anonymously or otherwise, by telephone or by telegraph, mail or any other form of written communication, in a manner likely to cause annoyance or alarm...” (§240.30 Penal Law of the State of New York). Users are advised of the statute and the consequences. Any such use will be deemed a violation of school policy.

2. **Privileges.** The use of the Internet is a privilege, not a right, and inappropriate use may result in a forfeiture of those privileges. The system administrator, oversight committees and Board of Education will deem what is appropriate use and their decision is final. Also, the system administrator may close an account at any time as required, not necessarily as a result of misuse, which may result in temporary loss of Internet access. The administration, faculty, and staff of the Hamilton Central School District may request the system administrator to deny, revoke, or suspend specific user accounts based on review of a specific incident or identified pattern of misconduct.

3. **Liability.** The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages users suffer. This include loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions caused by its own negligence, negligence on the part of operators or users of other networks.
connected to the Internet, or user errors or omissions. Use of any information obtained via the Internet is at the user’s risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through use of its services.

4. Rules Governing Internet Use. Users are expected to abide by the generally accepted rules for Internet use. These include, but are not limited to, the following:

- Never reveal personal information about yourself (e.g., home address, age, phone number, etc.) or that of students or colleagues.
- Note that electronic mail (e-mail) is not guaranteed to be private. Personnel who operate the system have access to all mail. Messages discovered to be relating to or in support of illegal activities are subject to administrative review and will be reported to the authorities.
- Be polite. Abusive, discriminatory, or defamatory messages will not be tolerated. Use appropriate language. Do not swear, use vulgarities or any other inappropriate language. Illegal activities are strictly forbidden.
- Attempting to override filtering/blocking software by way of proxy sites or other means is strictly forbidden.

5. Security. Security on any computer system is a high priority, especially when the system involves many users. If you feel you can identify a security problem on the local network or Internet, you have an obligation to notify a system supervisor. Do not demonstrate the problem to other users. Additionally, keep your user account information secret; never share this personal information, use another individual’s account, or attempt to discover, alter, or distribute such information. Attempts to log on to any network as a system administrator will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to local networks as well as the Internet.

6. Vandalism. Vandalism will result in the immediate forfeiture of all privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any of the above listed agencies or other networks that are connected to the Internet backbone. This includes, but is not limited to, the uploading or creation of computer viruses, Trojan horses, worms, or their variants.

The District reserves the right to limit and/or terminate Internet access privileges in the event it determines that an individual has violated this or any other policy or regulation of the District, or of any state or federal law, or that such person has otherwise utilized the District’s Internet access in an inappropriate or irresponsible manner.

Electronic Mail Responsible Use

Hamilton Central School 2017
1. **Purpose.** The District maintains an electronic mail (e-mail) system for educational purposes as well as for the purpose of conducting school business. This policy governs the use of that e-mail system. Policy on Internet access is incorporated herein by reference and will apply to employees and student use of the District’s e-mail system to the extent not superseded by this policy.

2. **Ownership and Privacy.** The electronic mail system, including data files and electronic storage areas, is the property of the District and is subject to District control and inspection. All messages composed, sent, or received on the e-mail system are the property of the District. The District may access or disclose any electronic messages or files for purposes including, but not limited to, the need to protect system security, fulfill District obligations, detect employee wrongdoing, comply with legal process, or protect the rights or property of the District, staff, students, or community. Electronic mail is not private, and messages relating to confidential information may be disclosed. Moreover, messages relating to or in support of illegal activities will be reported to the authorities.

3. **Security.** Employees are cautioned that the use of passwords for security does not guarantee confidentiality. Care should be taken when sending or retrieving sensitive, personal information across the e-mail system. Messages should be treated as confidential, and accessed only by the intended recipient. Employees are directed not to read or attempt to retrieve any e-mail messages that are not sent to them. The superintendent of schools or his designee is authorized to retrieve and review any and all e-mail messages.

4. **Usage.** The use of the e-mail system is intended for educational purposes and District business. Limited, occasional or incidental use of the e-mail system (sending or receiving) for personal, non-business purposes is understandable and acceptable to the extent that there is no tangible cost to the District nor any negative impact on the District’s computer or network resources. Use of the e-mail system to conduct matters related to personal companies, commercial ventures, or home-based businesses (i.e. lawn care service, direct marketing, consulting, etc.) is strictly prohibited (see Content section below). The user is responsible for his or her actions in accessing network services. System users are prohibited from creating, receiving, uploading, downloading, and/or transmitting inappropriate material. Inappropriate material includes, but is not limited to, that of a lewd, lascivious, pornographic subject matter.

5. **Content.** The e-mail system may not be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other solicitations unrelated to the District. The e-mail system is not to be used to create or distribute messages that address age, sexual orientation, beliefs, national origin, or disability in a manner that a reasonably prudent person might find to be offensive. The e-mail system shall not be used to send (upload) or receive (download) copyrighted materials, trade
secrets, proprietary financial information, or similar materials without consent of the owner of the information.

6. **Archived Files.** The District reserves the right to set quotas and retention periods for message storage as necessary to maintain optimum system integrity and performance. The confidentiality of any message should not be assumed. Even after a message is erased, it may still be possible to retrieve and read that message.

7. **Consequences.** Violations of this policy should be promptly reported. Use of the e-mail system is a privilege, not a right, and inappropriate use as determined by the system administrator may result in revocation of that privilege, or other disciplinary measures, up to, and including discharge or expulsion. The system administrator may close an account at any time at his or her discretion. The administration, faculty and staff at any school location may request the system administrator to limit, deny, revoke, or suspend user accounts, and the system administrator may act accordingly.

8. **Student E-Mail.** Student email accounts may be provided per teacher request for specific class projects. In addition to the above, students are prohibited from revealing or disseminating personal information about themselves (e.g., full name, home address, age, phone number, etc.) or that of other students or colleagues except in approved curricular activities that are supervised or moderated by teachers or other District staff.

9. **School District Oversight.** E-mail activity may be monitored by the District. Thus, there is no basis for an expectation of personal privacy regarding e-mail use.

**Internet Safety**

In accordance with The Children’s Internet Safety Act (CIPA), the District will enforce a policy of Internet safety that includes the use of technological measures and direct supervision as indicated in the preceding portions of this document.

The District has, and will maintain, Internet filtering/blocking services and/or software that are set to protect against access to material through District computers that is obscene, pornographic or in other ways harmful to minors. Students and staff that find appropriate materials are being blocked or that inappropriate material can be accessed, should report such problems immediately so that the filtering/blocking services may be adjusted accordingly. The school also has and will maintain hardware and/or software that have the capability of controlling access to direct electronic communication mediums such as “chat rooms.” The District has, and will maintain, the ability to monitor use of school computer use, both electronically and by direct supervision when it is deemed necessary to help prevent access to inappropriate material, promote safety for users, control access to direct electronic...
communications such as “chat Rooms” and e-mail, and prevent and detect “hacking” or other unauthorized use.

In accordance with the requirements of CIPA, all district computers connected to the Internet will be subject to the above filtering, blocking and monitoring measures, whether used by students or adults. CIPA allows for filtering to be overridden during use by adults engaged in “bona fide research.” Adults who wish to use the District’s computer system for research requiring that filtering/blocking be overridden should direct their requests to the Director of Technology who will determine if such request should be honored. Should the Director of Technology deny a request, the adult making the request may appeal to the Superintendent of Schools.

As indicated previously in this document, students using e-mail and the Internet are prohibited from revealing or disseminating personal information about themselves (e.g., full name, home address, age, phone number, etc.) or that of other students or colleagues except in approved curricular activities that are supervised or moderated by teachers or other District staff.
Hamilton Central School District  
Opt-Out Policy for Publishing Student Photographs and Student Work on the Hamilton Central School District Websites and in District-Related Publications

During the course of the year, your child’s name, work and/or image may be selected to highlight his or her accomplishments for publication on our website, on a teacher-created website linked to the district’s site or on other District media communications. The District believes that there is significant educational value in sharing these accomplishments. We feel it enhances communications between home and school, it extends learning opportunities beyond the classroom and creates a sense of pride for students.

Opt-Out Option: Parent Written Request Not To Publish Student Image
A parent or eligible student may request that their child’s name, work or image not be published. Such requests must be made in writing and sent to your child’s school annually. If you have questions concerning this policy, please contact the principal of the building your child attends.

Hamilton Central School District  
Opt-Out Policy for Non-Instructional Internet Access

As part of the instructional process, internet access is available to students and teachers in the Hamilton Central School District. Our primary goal in providing this service to teachers and students is to promote educational excellence in schools by facilitating research, resource sharing, innovation, and communication.

Hamilton Central School District will take precautions to restrict access to controversial materials. However, on a global network it is impossible to control all materials and a user may discover controversial or objectionable information. The use of the Internet is a privilege, not a right, and inappropriate use may result in a forfeiture of those privileges and or other disciplinary procedures. All users of the District’s internet services must abide by the District’s Acceptable Use Policy, located at www.hamiltoncentral.org under Departments, Instructional Technology, Technology Plan & AUP (please review).

The Hamilton Central School District firmly believes that the valuable information and interaction available on this worldwide network far outweighs the possibility that users may procure material that is not consistent with the educational goals and philosophies of the District. Therefore, the Internet is a valuable resource and may be used by students during instructional time and during non-instructional time, such as study halls.
Opt-Out Option: Parent Written Request to Deny Internet Access During Non-Instructional Time

If a parent chooses not to allow their child to have access to the internet during non-instructional times, such requests must be made in writing and sent to your child’s school annually. If you have questions concerning this policy, please contact the principal of the building your child attends.