

Hamilton Local School District
Computer Network and Internet Acceptable Use Policy

The Hamilton Local School District (the "School District") is pleased to make available to each student access to interconnected computer systems, computer equipment, computer programs, the Internet, electronic mail and other new technologies within the School District (collectively, the "Network").

Access to the School District's Network is provided as a privilege and as an educational tool only. In order to continue enjoying access to the Network, users must take responsibility for appropriate and lawful use of this privilege. Users are responsible for good behavior on the Network just as they are in a classroom, school hallway or other School District property. While the School District's teachers and other staff may make reasonable efforts to supervise student use of Network access, the ultimate responsibility for exercising and promoting responsible use of this access is that of the student and the parent/guardian.

This shall constitute the School District's Computer Network and Internet Acceptable Use Policy for Students and Staff ("Policy"). A copy of this Policy shall be provided to staff, students and parents/guardians. Any parent/guardian of a student under the age of 18 may direct that the student not be given access to the Internet. An "opt out" form for this purpose may be obtained from the School District.

Each user is responsible for reading and abiding by this Policy. If you have any questions about the provisions of this Policy, you should contact the Computer Lab Facilitator or other designated administrator in your school building. Any use of your account that violates this Policy may result in your access being withdrawn and/or additional disciplinary action. Users and parent/guardians should be familiar with the Student Discipline Code (the "Student Discipline Code") and the District's Board Policies. Violations of this Policy are considered violations of the Student Discipline Code and the District's Board Policies and may result in disciplinary action as specified therein.

1. Reporting Misuse of the Network

In addition to following the terms of this Policy, you should report any misuse of the Network to the person designated by the School District for this reporting. Misuse means any violations of this Policy or any other use that is not included in this Policy but has the intent or effect of harming another or another's property.

2. Term of the Permitted Use

Access to the Network is a privilege, not a right, and as such it may be suspended or revoked by the School District at any time for technical, policy, or other reasons. Users have no privacy expectation in the contents of their personal files or any of their use of the District's network or equipment within. The District reserves the right to monitor, track, log, and access all use and/or communications created within, including employee's, student's, and guest's personal computers, network, Internet, electronic communications, and media brought onto School District property or at School District events. This includes, but is not limited to video, images, audio files, or any other electronic data. Access to all data on, taken from, or compiled using the School District's network, computers or electronic devices is subject to inspection and discipline. The School District may also limit access depending on student and staff schedules and equipment availability.

3. Access

Network resources are only intended for use by authorized users. Anonymous use is not permitted, and access may not be shared or transferred. Users shall not share their passwords or otherwise allow anyone to gain unauthorized access to the Network or the Internet. A user is subject to disciplinary action under Board Policy and/or the Student Discipline Code for any violations of this Policy committed by someone else who, with the user's express or implied permission, accessed the Network with the user's password.

4. Purpose and Use

The School District is providing you access to its Network **only** for educational purposes. For this reason, the following acceptable and unacceptable use guidelines must be understood and followed. If you have any doubt about whether a contemplated activity is educational, you may consult with the Computer Lab Facilitator or another person designated by the School District to help you decide if a use is appropriate.

Employees' and students' must understand that personal technology devices brought onto the School District's property, may be legally accessed, if suspected they contain School District information and/or are a possible violation of District Policies, in order to insure compliance with School District policies, to protect the District's resources, and to comply with the law. Users may not use their personal computers, cell phones (with or without Internet access and/or recording and/or camera and other capabilities), or any other electronic device to access the District's Intranet, Internet, or any other

District systems, unless approved by the District's Administration. In accordance with Board Policy, cellular phones and certain electronic equipment (ex. iPods) are permitted at specified times and in specified areas, however, these devices must use their carrier network. District-owned Internet use (wired or wireless) by these types of devices is prohibited, unless express written permission has been obtained from building or district Administration.

5. User Responsibilities

- Students and employees of the Hamilton Local School District are responsible for acceptable, appropriate, and legal use of the district's network.
- All District Policies and Rules contained in this document, Board Policy, and in the Student Code of Conduct must be followed at all times.

6. Acceptable Uses of the Internet:

- To support learning
- Inform/Enlighten
- Research educational topics
 - *When conducting research, students should stick to the topic and evaluate the usefulness of the data. (Elementary): Stay on sites that have been bookmarked for you. If "searching" is needed, seek the assistance of a teacher.
- Communicate with others for the purpose of learning
- Practice curricular skills

7. Instant Messaging, Email and Communication Netiquette

E-mail and Instant Messaging are communication tools, which allow students to communicate one-to-one with people throughout the world. Students may have e-mail or instant messaging access only under their teacher's direct supervision using a classroom account. Students may be provided with individual e-mail or communication accounts under special circumstances, at the request of their teacher. Students may not establish web e-mail accounts through the Hamilton Local School's network (for example, AOL email, Hotmail, YahooMail, etc, or any Instant Messaging Service).

All users must abide by the rules of Network etiquette. Among the uses and activities that violate Network etiquette and constitute a violation of this Policy are (but not limited to) the following:

- (a) Using inappropriate language, including swearing, vulgarities or other language that is suggestive, obscene, profane, abusive, belligerent, harassing, defamatory or threatening. Users must be polite: No FLAMMING, SCREAMING, demeaning or other inappropriate communications.
- (b) Using the Network to make, distribute or redistribute jokes, stories or other material that would violate this Policy or the School District's harassment or discrimination policies, including material that is based upon slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, sexual orientation or other protected characteristics.
- (c) Forwarding or redistributing the private message of an e-mail sender to third parties or giving the sender's e-mail address to third parties without the permission of the sender.
- (d) Sending e-mail attachments that are too large to be accommodated by the recipient's system.
- (e) Communications that violate any District Policy or the law.

8. Unacceptable Uses

The Board or authorized School District officials will make a good faith judgment as to which materials, files, information, software, communications and other content and activities are permitted and prohibited under the particular circumstances based on the following guidelines. Among the uses and activities that are considered unacceptable and constitute a violation of this Policy, the following are (but not limited to) prohibited:

- (a) Uses or activities that violate the law, Board Policy, or the Student Discipline Code, or that encourage others to violate the law, Board Policy, or the Student Discipline Code. Among such uses or activities (but not limited to) are the following:
 - (i) Offering for sale or use any substance the possession or use of which is prohibited by law, Board Policy, or the Student Discipline Code.

- (ii) Creating, copying, viewing, transmitting, downloading, uploading or seeking sexually explicit, obscene or pornographic materials. This includes sexting (the act of sending sexually explicit messages or photos electronically, primarily between cell phones).
 - (iii) Creating, copying, viewing, transmitting, downloading, or uploading any materials that include the design or detailed information for the purposes of creating an explosive device, materials in furtherance of criminal activities or terrorist acts, threatening materials or any other materials that violates or encourages others to violate the law, Board Policy, or the Student Discipline Code.
 - (iv) Unauthorized copying, modifying, intruding, or attempts to copy, modify or intrude, into the folders, files, data, work, networks, passwords or computers, or electronic devices of others, or intercepting communications intended for others.
 - (v) SPAMMING or distributing chain letters. (SPAMMING is sending an annoying or unnecessary message to a large number of people.)
 - (vi) Copying, downloading, uploading or transmitting confidential information or trade secrets.
- (b) Uses or activities that cause harm to others or damage to their property. Among such uses or activities are (but not limited to) the following:
- (i) Uploading, downloading, creating or transmitting a computer a virus, worm, Trojan horse, or other harmful component or corrupted data, or vandalizing the property of another. Vandalism includes any malicious attempt to hack, alter, harm or destroy software, hardware, data of another user, other Network resources, or the use of the Network to destroy anything on the Internet or outside Networks.
 - (ii) Uploading, downloading, copying, redistributing or republishing copyrighted materials without permission from the owner of the copyright. Even if materials on the Network are not marked with the copyright symbol, you should assume that they are protected under copyright laws unless there is explicit permission on the materials to use them. Violations of copyright law can be a felony and the law allows a court to hold individuals personally responsible for infringing on the law. The School District does not permit illegal acts pertaining to copyright law. Therefore, any user violating the copyright law does so at their own risk and assumes all liability. Violations of copyright law include, but are not limited to, the making of unauthorized copies of copyrighted material (such as commercial software, text, graphic images—including photos, audio and video recordings.), All material posted on the district web site (including images) are the property of the district and protected as such. Employees or students who post to class, department, or athletic websites linked to, or as a part of the district website must follow all copyright laws. Additionally, students and staff are not permitted to plagiarize material accessed through the School District's systems/network.
 - (iii) Posting or distributing inappropriate photos or media (pornography, dangerous, or hate-related media of any kind.) This includes cyberbullying or harassing another individual (student or employee) or posting/transmitting information of any kind about another person without their consent, including, but not limited to video, images, audio, text, or any other media. Example: Any material, images/media taken from within the district or it's property cannot be used for defamatory, inaccurate, obscene, sexually explicit, lewd, hateful, harassing, discriminatory, violent, vulgar, rude, inflammatory, threatening, profane, pornographic, offensive, or terroristic purposes. This includes, but is not limited to, disseminating electronically (email/Instant Messaging) or posting this type of information about another student or employee on an outside communication site such as MySpace, FaceBook, etc.
 - (iv) Using another's password or some other user identifier that misleads message recipients into believing that someone other than you is communicating or otherwise using the other's access to the Network, this includes altering a communication or image originally received from another person, computer, or any electronic device with the intent to deceive.
 - (v) Defaming another (such as harming their reputation by lies). This includes the use of inappropriate language (profanities, obscenities, or other language including threats, attacks on race, national origin, sexual orientation, age disability, political beliefs, or sexual explicitness that may be considered as harassment). This includes, but is not limited to, disseminating electronically (email/Instant Messaging) or posting this type

of information about another student or employee on an outside communication site such as MySpace, FaceBook, etc.

- (vi) Students or employees may not invade one's privacy by disclosing, or the using, or disseminating confidential and/or personal information. (Examples include, but are not limited to, using a cell phone with camera and Internet access to take pictures of anything, including but not limited to, persons, places, and documents relevant to the School District, saving, storing, and sending the image with or without text or disclosing them by any means, including but not limited to, print, and electronic matter; revealing students grades, any personal information, or records, unless legitimately authorized to do so by a District Administrator.)
- (vii) Social Networking Web Sites:
 - 1. District Staff members and students who personally participate in social networking web sites are prohibited from posting data, documents, photographs, or inappropriate information on any web site that might result in a disruption of classroom or District activity. The Superintendent/designee has full discretion in determining when a disruption of classroom or District activity has occurred.
 - 2. District staff is prohibited from providing social networking web site passwords to students.
 - 3. Fraternalization between district Staff and students via the Internet, personal email accounts, social networking web sites, and other modes of virtual technology is also prohibited.
 - 4. Access of social networking web sites during school hours is prohibited.Violation of the prohibitions listed above will result in staff and/or student discipline in accordance with State law, Board policies and regulations, the Student Code of Conduct and/or staff negotiated agreements. Nothing in this policy prohibits District staff and students from the use of education web sites.
- (c) Commercial uses. For example, do not sell or buy anything over the Internet (such as from eBay or Amazon), do not solicit or advertise the sale of any goods or services (whether to one recipient or many, such as "junk e-mail"), and do not give others private information about yourself or others, including credit card numbers or social security numbers.
- (d) Uses or activities that are unrelated to the curriculum (e.g., surfing the Internet, playing games). Users shall not use the Network to access chat rooms or chat lines. All use of e-mail and instant message collaboration must be through the School District's e-mail service.
- (e) Uses that degrade or disrupt the operation of the Network or that waste limited resources. For example, do not waste toner or paper in printers, and do not send chain letters, even for non-commercial or apparently "harmless" purposes, as these, like "junk e-mail," use up limited Network capacity resources.
- (f) Uses that violate the standards of academic integrity, including but not limited to plagiarism.
- (g) Suggesting to other's that they view, download or seek materials, files, information, software or other content that may be offensive, defamatory, misleading, infringing or illegal.
- (h) Installing or downloading software or hardware without the prior consent of a School District administrator. Users may not move, repair, reconfigure, modify or attach any external devices to Network equipment, computers or systems. Users shall not remove, alter or copy Network software for their own personal use or for the use of others.

9. Internet Safety/Guidelines Regarding Network or Internet Use

- (a) General Warning. All employees, students and their parents/guardians are advised that access to the Network and particularly the Internet may include the potential for access to materials inappropriate for school-aged pupils, including materials that may be illegal, defamatory, obscene, inaccurate or offensive. Certain of these areas on the Internet may contain warnings as to their content, and users are advised to heed these warnings. Not all sites that may contain inappropriate material, however, will include warnings. You must take responsibility for your use of the Network and stay away from these sites. Parents/guardians of minors are the best guide to the materials to avoid. If you find that other users are visiting offensive or harmful sites, you should report that use to the person designated by the School District. If you should mistakenly access inappropriate information, you should immediately tell your teacher or supervisor to protect yourself against a claim of violating this policy.

- (b) System Security: You are responsible for your individual account and must take all reasonable precautions to prevent others from being able to use your account. Under no conditions should you provide your password to another person. You will immediately notify a supervisor, teacher or the system administrator if you have identified a possible security problem. Do not go looking for security problems, because this may be construed as an illegal attempt to gain access.
- (c) Personal Safety. Be safe. Do not use the Network or the Internet to access chat rooms or chat lines. In using the Network or the Internet, do not reveal personal information such as your or another's home address, telephone number, social security number or photograph. Due to the anonymous nature of the Internet, students should not arrange a face-to-face meeting with someone you "meet" through the Network or the Internet without permission of your parent or guardian. If you receive any communication that makes you uncomfortable or is inappropriate, you should immediately tell your teacher or another school employee.
- (d) Confidentiality of Information. Personally identifiable information concerning employees or students may not be disclosed or used in any way on the Network without the permission of the employee, a parent/guardian or, if the student is 18 or over, the permission of the student himself/herself. Users should never give out private or confidential information about themselves or others on the Internet. A supervising teacher or administrator may authorize the release of directory information, as defined by Ohio law, for internal administrative purposes or approved educational projects and activities.
- (e) Active Restriction Measures. Consistent with applicable law, the School District, either by itself or in combination with the Data Acquisition Site providing Internet access, will utilize filtering software or other technologies to limit student access to visual depictions that are (1) obscene, (2) child pornography, (3) harmful to minors, or (4) otherwise objectionable. The School District will also monitor the online activities of students, through direct observation and/or technological means, to limit student access to such depictions or any other material which is inappropriate for minors. As it is impossible to limit access to all materials that may be considered inappropriate, the ultimate responsibility for monitoring Network usage is that of the student, and the student's parents/guardians.

Internet filtering software or other technology-based protection systems may be disabled by a supervising teacher or school administrator, as necessary for purposes of bona fide research or other educational projects being conducted by students age 17 and older.

The term "harmful to minors" as used herein shall have the same meaning as defined in the Communications Act of 1934 (47 USC Section 254 [h][7]).

10. Privacy

Network access is provided as a tool for education. The School District reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the Network and any and all materials, files, information, software, communications (including emails) and other content transmitted, received or stored in connection with this usage. All such information, content and files shall be and remain the property of the School District and you should not have any expectation of privacy regarding those materials. Network administrators may review files and intercept communications for any reason, including but not limited to for purposes of maintaining system integrity and ensuring that users are using the system consistently with this Policy.

11. Web Sites

Web sites created through the Network and/or linked with the School District's official web site must relate specifically to District-sanctioned activities, programs or events. Web sites created using the Network or the School District's equipment, or web sites created as part of a classroom or club assignment or activity are the sole and exclusive property of the School District. The School District reserves the right to require that all material and/or links with other sites found to be objectionable be altered or removed. All external web sites linked with any School District web page must prominently display the following disclaimer:

This is not an official web site of the Hamilton Local School District. The Hamilton Local School District does not control and cannot guarantee the timeliness or accuracy of the information on this web site. Any views or opinions expressed herein are solely those of the creators of this web site.

As appropriate, the School District may also require such disclaimer on other external web sites that relate directly to School District activities, programs or events.

12. Failure to Follow Policy

Your use of the Network is a privilege, not a right. If you violate this Policy, you may be subject to disciplinary action. At a minimum you will be subject to having your access to the Network terminated, which the School District may refuse to reinstate for the remainder of your enrollment in the School District. You breach this Policy not only by affirmatively violating the above Policy, but also by failing to report any violations by other users that come to your attention. A violation of this Policy may also be a violation of the law and subject the user to criminal or civil investigation and prosecution.

13. Warranties and Indemnification

The School District makes no warranties of any kind, either express or implied, in connection with its provision of access to or use of its Network. It shall not be responsible for any claims, losses, damages or costs (including attorneys' fees) of any kind suffered, directly or indirectly, by any employee, student, or parent/guardian arising out of the use of, or inability to use, the Network. Each user is responsible for backing up his or her files. The School District is not responsible for the accuracy of information obtained through electronic information resources, and this information should be used at the user's own risk.

By accessing the Network, you (or, if you are a minor, your parents/guardians) are agreeing to cooperate with the School District in the event of the School District's initiating an investigation of use or access to the Network through your account, whether that use is on a School District computer or on another computer, or electronic device outside of the Network. By accessing the Network, you (or, if you are a minor, your parents/guardians) are further agreeing to indemnify and hold the School District and the Data Acquisition Site and all of their administrators, teachers and staff harmless from any and all loss, costs, claims or damages (including attorneys' fees) resulting from access to and use of the Network through your account, including but not limited to any fees or charges incurred through purchases of goods or services by the user.

14. Limitation of Liability

The District makes no guarantee that the functions or the services provided by or through the District system will be error-free or without defect. The District will not be responsible for any damage you may suffer, including but not limited to, loss of data or interruptions of service. The District is not responsible for the accuracy or quality of the information obtained through or stored on the system. The District will not be responsible for financial obligations arising through the unauthorized use of the system. Users, (or, if you are a minor, your parents/guardians) can be held financially responsible for any harm to the system as a result of intentional misuse.

15. District Equipment taken off District Property

Hamilton Local Schools must execute property accounting procedures designed to ensure the accuracy of records regarding the acquisition, maintenance, control and disposition of equipment and property. Under certain circumstances, Hamilton Local Schools will permit checkout of equipment for use on--or in some cases off the property for completion of academic, teaching, or administrative assignments. Individuals borrowing Hamilton Local School's equipment assume full responsibility for the care and security of such property.

A combination of accurate accounting records and strong internal controls must be in place in order to detect and protect against loss and unauthorized use of Hamilton Local School's property. Individuals borrowing property of Hamilton Local Schools from the Technology Department or Library are required to complete the appropriate documentation, so that equipment inventories will accurately reflect the disposition of all the property of Hamilton Local Schools.

RESPONSIBILITIES:

Equipment loaned out for use during or outside of the school day with the authorization the appropriate Department Head is the responsibility of that employee or student who borrows the item. Loss or damage due to negligence (such as leaving a laptop, camera or any other equipment laying around unattended) may result in a charge to that individual of the replacement cost of the item. Any faculty, staff, or student checking out equipment (for either "on-site" or overnight use) will be personally responsible and liable for its safeguard and return in serviceable condition. Individuals who cause damage or loss, or who have an item stolen, will be charged the full purchase cost of replacement equipment. Any replacement or repair costs will automatically be applied to the payroll statement of an employee (faculty or staff). Therefore, it is recommended that borrowers check with their insurance company to ensure the equipment is covered by their personal policy while off school grounds.

In case of such loss while in the possession of a student, the authorizing person may ask the student to pay this amount to the school. For equipment checked out to **students** for **overnight use**, the form that must be signed by the parent/guardian specifies that they are assuming financial responsibility for the item-- and can be held liable for *any* loss or damage to the item (normal wear out or equipment breakdown not included).

In all cases, the equipment is to be returned upon completion of the designated project, or any time at the discretion of the Technology Coordinator and/or Library Media Specialist, or any district administrator for any reason.

16. Updates

You, and, if appropriate, your parents or guardians, may be asked from time to time to provide new or additional registration and account information to reflect developments in the law or technology. You (or your parents or guardians) must provide this information in order for you to continue receiving access to the Network. If, after you have provided your account information, some or all of the information changes, you must notify the Computer Lab Facilitator, an Administrator, or other person designated by the School District to receive this information



KEEP THIS COPY FOR YOUR RECORDS

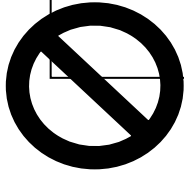
Adoption Date: May 11, 2009

Student: _____

(Please Print Clearly)

Grade: _____

Teacher: _____



DENIAL of Permission For Internet Access By Parent/Guardian



I have reviewed the Hamilton Local School District Computer Network and Internet Acceptable Use Policy for Students, which describes the terms of student access to interconnected computer systems, computer equipment, computer programs, the Internet, electronic mail and other new technologies.

*Full/Detailed Policy available online at: http://www.hamilton-local.k12.oh.us/Downloads/HamiltonAUP_ES2.pdf and http://www.hamilton-local.k12.oh.us/Downloads/HamiltonAUP_IS-MS-HS.pdf or in any of the building Offices.

As the parent of a student who is under the age of 18, I DO NOT wish the undersigned student to have access to the Internet via the School District's computer network. By signing below, I understand and agree that the undersigned student:

- May be required to complete alternate assignments as a result of this denial of permission for Internet access;
- May still have access to interconnected computer systems, computer equipment, computer programs, electronic mail and other new technologies within the School District other than Internet; and
- Will be obligated to comply with all remaining terms of Board Policy EDE – Students (i.e., those that do not relate directly to Internet access).

I further understand and agree that while the School District will undertake reasonable measures to ensure that the undersigned student does not access the Internet via the School District's computer network, it is not technologically feasible to guarantee that such access will be preventable under all circumstances. As such, I understand and agree that the ultimate responsibility for ensuring that the undersigned student does not access the Internet via the School District's computer network is that of myself (as the parent/guardian) and the undersigned student.

Name of Student (Print clearly)

Name(s) of Parent/Guardian

Address

Signature(s) of Parent/Guardian

Date

Signature of Student

Date

By signing this form, I am indicating my desire that my son/daughter WILL NOT have access to the Internet via the School District's Computer Network.



Student: _____ <i>(Please Print Clearly)</i>	Grade: _____
Teacher: _____	

Student Computer Use and Rules for Online Safety
(Elementary Version)
Hamilton Local Schools

1. I will respect all computer equipment and the network. I will not damage equipment or the network in any way. I (along with my parents) understand that I will be responsible for any and all damage that my improper use may cause. Any and all damage that results from my careless actions will result in disciplinary action as outlined in the Student Code of Conduct and any financial costs in repair of damages will be the responsibility of my parents and/or guardian.
2. I will not use or copy the work of another person without their permission. This is called plagiarism. Plagiarism is taking the ideas or writings of others and presenting them as if they were yours. If you use the work of someone else (research or pictures, for example), you must follow district guidelines regarding proper citation of this work.
3. I will not give out personal information such as my picture, address, telephone number, parents' work address/telephone number, or the name and location of my school without my parents' permission.
4. Even though the Internet network is "filtered" electronically to block possible inappropriate material, I will tell my teacher and/or parents right away if I come across any information that makes me feel uncomfortable.
5. I will follow the school rules for going online. I will not access inappropriate sites or break these rules.
6. I will be a good online citizen and not do anything that hurts other people or is against the law.
7. When conducting research, I will stick to the topic and read the information to evaluate it for usefulness.
8. I will stay on sites that have been bookmarked for me by educators in building. If "searching" is needed, I will seek the assistance of a teacher.

By signing this document, I acknowledge that I have read and discussed with my parents the above Online Rules and the "**Computer Network and Internet Acceptable Use Policy**", including Internet Safety/Guidelines Regarding Network or Internet Use, Uses of the Internet, Privacy, Failure to Follow Policy, and Limitation of Liability specified by the Hamilton Local Schools Acceptable Use Policy. I understand them and will follow these rules and guidelines at all times. If I break a rule, I understand that I may lose my online privileges and/or face disciplinary actions according to the Student Code of Conduct, Failure to Follow Policy, and/or the law.

*Full/Detailed Policy available online at: http://www.hamilton-local.k12.oh.us/Downloads/HamiltonAUP_ES2.pdf or in any of the building Offices.

Student Signature

Parent Signature (consent granted)

Date: _____

Building: _____

