Internet Safety & Acceptable Use Policy for

Clinton Community Unit School District 15

I. Introduction

It is the policy of the Clinton Community Unit School District 15 (hereafter Clinton School(s) or the District) to:
1. prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, chat rooms, or other forms of direct electronic communications;
2. prevent unauthorized access and other unlawful online activity;
3. prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and
4. comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

Additionally, access to the district network and the Internet provided by Clinton Schools is a privilege, not a right, and is expected to be used as an educational and/or work-related resource. Such access shall be made available subject to any and all rules and regulations that may be established. No use shall be permitted which, in the judgment of school administrators, is in any way prejudicial to the best interests of the District or is in conflict with the District's mission.

Clinton School administrators reserve the right to refuse access to the network or the Internet through the District to anyone when deemed necessary to the public interest.

II. Definitions

1. Access to the Internet – A computer or digital device shall be considered to have access to the Internet if such computer or digital device is equipped with a modem or is connected to a network which has access to the Internet.

2. Minor – The term "minor" means an individual who has not attained the age of 17.

3. Technology Protection Measure – The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:
   a. obscene, as that term is defined in section 1460 of title 18, United States Code;
   b. child pornography, as that term is defined in section 2256 of title 18, United States Code; or
   c. harmful to minors.

4. Harmful to Minors – The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:
   a. taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

b. depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
c. taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

5. Sexual Act; Sexual Contact – the terms "sexual act" and "sexual contact" have the meanings given such terms in section 2246 of title 18, United States Code.

6. Hacking – the term "hacking" shall mean any attempt to gain unauthorized access to any computer, digital device, or network system.

7. Authorized Staff Member – the term "authorized staff member" shall refer to any adult staff member appointed by the Clinton Schools Technology Team.

8. Technology Team – the term "technology team" shall refer to a group of the Clinton Schools staff including administrators, district technology staff, and staff appointed by building administrators.

III. Access to Internet by Minors

Minors using Internet services provided by Clinton Schools shall be subject to the following rules and regulations:

1. Minors shall not access materials that are obscene, child pornography, harmful to minors, or otherwise inappropriate for education, as determined by local standards.

2. Minors shall not use Clinton School Internet resources to engage in hacking or attempts to otherwise compromise the security of any computer, digital device, or network system.

3. Minors shall not engage in any illegal activities on or through the Internet.

4. Minors should only use the Internet, electronic mail, chat rooms, and other forms of direct electronic communications for purposes related to education within the context of a school's related assignment activity.

5. Minors shall not disclose any personal identification information regarding themselves or anyone else on the Internet.

IV. Access to Internet by Adults

Adults accessing Internet services provided by Clinton Schools shall be subject to the following rules and regulations.

1. Adults shall not access material that is obscene, child pornography, or otherwise inappropriate for training or work-related uses, as determined by local standards.

2. Adults shall not use Clinton School Internet resources to engage in hacking or attempts to otherwise compromise the security of any computer, digital device, or network system.

3. Adults shall not engage in any illegal activities on or through the Internet.

V. Technology Protection Measure

Clinton Schools shall employ a technology protection measure that blocks and/or filters Internet access to prevent access to materials that are obscene, child pornography, harmful to minors, or otherwise inappropriate for education, as determined by local standards. The use of such a technology protection measure does not preclude the necessity for staff to supervise student use of technology.

1. The technology protection measure may be disabled by the technology department for an adult user's bona fide research purposes with permission of the immediate supervisor of the staff member requesting said disabling or with the permission of District technology staff.

2. The technology department may override the technology protection measure for a minor to access a particular Internet resource for bona fide research or other lawful purposes during which time the minor will be monitored directly by a Clinton School staff member.

VI. Education about Appropriate On-Line Behavior

1. School district staff will educate students about appropriate online behavior, both in specific computer and digital device usage units and in the general curriculum.

2. Staff will specifically educate students on:
    a. appropriate interactions with other individuals via social networking websites, chat rooms, instant messaging, email, and other forms of direct electronic communications; and
    b. cyberbullying awareness and response.

VII. Web Page Creation Guidelines

Web pages may not contain any personal business or inappropriate content. Web pages are subject to revision or removal at the discretion of the District technology staff and/or administration.

In addition, all Clinton School web pages must comply with the following guidelines:

1. must not include photos, videos, or audio of any student unless they have a current Photography & Video Release Form on file;

2. must not display students' last names; and

3. must not display students' email addresses.

VIII. Email Guidelines

Clinton Schools will make email accounts available to students and staff for educational purposes. Teachers may ask for classroom accounts or individual accounts for their students. Before receiving their passwords and account information for individual accounts, students must

attend an orientation session. Students are held responsible for any email sent under their user name, so passwords should be kept confidential.

IX. Inappropriate Use of Technology Resources

The following activities are examples of inappropriate activities for any Clinton School computer, digital device, network, email system, or the Internet. The list is not all-inclusive. Anything that would be considered inappropriate in "paper form" is also considered inappropriate in electronic form. District administration reserve the right to determine what is considered inappropriate by local standards.

1. Using another user's password or attempting to determine another user's password.

2. Sharing your own password with another.

3. Trespassing in another user's files, folders, home directory, or work.

4. Saving information on ANY network drive or directory other than your personal Home directory or a teacher specified and approved location.

5. Downloading or installing any software on any district device without proper approval.

6. Using any technology resources to harass, insult, or attack another.

7. Damaging any computer, computer equipment, digital device, or network (this includes changing workstation configurations such as screen savers, backgrounds, printers, BIOS information, preset passwords, etc.).

8. Intentionally wasting limited resources such as disk space and printing capacity.

9. Accessing inappropriate web sites (sites containing material related to violence, gambling, terrorism, sexual activities, other illegal activities, etc.)

10. Sending, displaying, or downloading offensive messages, images, or videos.

11. Using obscene, racist, profane, discriminatory, threatening, or inflammatory language.

12. Participating in chat rooms without the permission/supervision of an adult staff member.

13. Posting any false or damaging information about another person, the school system, or other organizations.

14. Posting any personal information about another person without his or her written consent.

15. Broadcasting network messages and/or participating in sending/perpetuating chain letters.

16. Violating trademark, servicemark, or copyright laws.

17. Plagiarism of materials that are found on the Internet.

18. Use of technology resources to create illegal materials (counterfeit money, fake identification, etc.)

19. Use of any Clinton School technology resources for personal gain, commercial or political purposes.

20. Accessing online audio and/or video without curricular justification. Audio and video transmission may slow down network services (access to Internet, email, library catalog, file servers, etc.) throughout the district.

X. Acceptable Use of Technology Resources

This policy governs the use of all Clinton School technology resources, including but not limited to computers, computer equipment, digital devices, networks, and district owned software. All Clinton School technology resources are to be used only by employees of Clinton Schools, students currently enrolled in Clinton Schools, and those people who have received the proper authorization from the District's technology staff and/or building administrators.

Use of the Clinton School technology resources is a privilege, not a right, and is provided to assist faculty, students, and other authorized users enhance their opportunity to learn and perform job functions. The District reserves the right to restrict, suspend, or completely revoke such use as it deems fit. Users must be aware of and comply with the following general rules:

1. Anyone using Clinton School technology resources shall act responsibly and respect the rights of others.

2. The Clinton School network and the Internet are to be used for educational purposes only, and all other uses (such as chatting, playing games, file sharing, streaming audio/video, etc.) are prohibited, unless authorized by administration or the technology staff.

3. Authorized users of email will not engage in spamming and will not create, post, send, or forward electronic chain letters. If anyone asks you to stop sending them email, you must obey the request. Email harassment will not be tolerated.

4. Any use of the network or the Internet for commercial purposes, advertising, or political lobbying is prohibited.

5. Software installation requests should be made 15 days prior to the first day the application is needed.

6. All software installation will be performed by or under the direct supervision of the technology department.

7. Any software installation performed without the technology department's approval will not be supported and may be removed.

8. Violation of copyright laws will not be permitted. Plagiarism of data on the Internet will not be tolerated, and installing illegally obtained or unlicensed software is prohibited. Any unauthorized content or applications will be removed without notice and criminal prosecution may result.

9. USB flash drives will not be permitted unless authorized by the technology department. Authorized users will have their computers configured to scan the drive for viruses prior to use.

10. No one shall knowingly or negligently damage, vandalize, "hack," alter, reconfigure, modify, or destroy school technology, either from within or outside school facilities. No alterations or changes shall be made to any technology (such as computer software configurations) without permission from the technology staff. Although the following list is not exhaustive, it exemplifies activities that shall be considered vandalism: printing excessive copies; attempting to "crash" computers or networks; creation, intentional use, or installation of unauthorized devices, objects, or programs; modification of technology resources, utilities, and configurations; attempting to change the restrictions associated with user accounts; attempting to breach any technology security systems. Staff and students will abide by state and federal laws related, but not limited to, computers, public information, and communication systems.

11. Users shall not assemble, disassemble, connect, or disconnect technology or network equipment unless authorized by the technology staff.

12. Users shall not move technology equipment or software to another location without prior consent of the technology staff.

13. All media used in school technology will first be scanned for viruses and malicious software by technology staff before being used.

14. District administrators and technology staff reserve the right to inspect any student's technology, data, and media used to access school technology to investigate or determine if a violation of the Internet Safety & Acceptable Use Policy has occurred. Students not willing to allow inspection will not be allowed to bring technology, data, and media to access school technology.

15. Individual account and password information must not be provided to others for use of the network. Unauthorized use of an account and password by anyone other than the account owner will not be allowed.

16. Clinton Schools, by providing network and email accounts, is in no way granting a user any sort of private or personal account. The District retains complete ownership of all its files stored on any system and may retake control of those files if it has reason to believe, in its sole discretion, that a user is in violation of the Internet Safety & Acceptable Use Policy.

17. Clinton Schools, by providing an account, is in no way authorizing a user to enter into any financial obligation or access any sites which require the user to pay a fee. The user may be personally responsible for any financial obligations entered into or incurred while using District-owned accounts and systems.

18. Users must follow all rules and guidelines developed by the technology staff. These rules and guidelines shall be posted at a designated place in each building and it is the user's duty to periodically review them.

19. Personal "Home" folders shall not exceed the size limitation determined by the technology staff. All outdated material must be removed from your personal "Home" folders. If outdated items are not removed in a timely manner they will be removed by the technology staff.

20. Staff may not allow student use of technology or network resources without supervision.

21. All District-issued technology shall remain in the accompanying District-issued protective cover, unless the technology staff grants authorization to move the equipment to another suitable protective cover. At all times school equipment must be in an approved protective cover. Repair or replacement of equipment broken while not in a protective cover will be the responsibility of the user.

22. Staff may not allow student use of technology or network resources that does not specifically relate to a curriculum or proficiency test outcome.

23. Users have a duty to report any improper use of Clinton School technology or network resources to the building administrators and/or technology staff. This includes the receipt of any email which recipient feels is inappropriate.

24. Building administrators reserve the right, at their sole discretion, to suspend or terminate a user's access to District technology or network resources, or to take whatever corrective actions they deem appropriate, for any misuse of the technology or network resources.

25. Users will document in writing, within 24 hours, any damage done to District technology resources. The documentation shall include time, location, and a detailed explanation of the events resulting in the equipment's damage.

XI. Policy Violations

Any violation of this policy by staff or students may result in the loss of access to the Internet and/or network by those individuals who are in violation. Additional disciplinary action may be taken in accordance with existing procedures and practices, both administratively and as stipulated in any Clinton Schools handbook or other technology policy guides, as well as including applicable law enforcement agencies when necessary.

XII. Policy Challenge Procedure

In the event that an individual challenges a decision made regarding this policy, that individual will be afforded all due process rights.

XIII. Adoption

This Internet Safety & Acceptable Use Policy was adopted by the Clinton Community Unit School District 15 Board of Education at a public meeting, following normal public notice, on December 18, 2012.