STUDENT ACCEPTABLE USE AND INTERNET SAFETY POLICY
For the Computer Network of the
FINDLAY CITY SCHOOL DISTRICT

Students are encouraged to use the school's computers/network and the Internet connection for teacher-assigned, educational work. All references to schools in this policy will mean any school in the Findlay City School District.

Access to the School District's Network is provided as an educational tool only. In order to continue enjoying access to the Network, each student must take responsibility for appropriate and lawful use of this privilege. Students 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 ("Policy"). 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 any school office in the School District.**

Each student 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 Any use of your account that violates this Policy may result in your access being withdrawn and/or additional disciplinary action. Violations of this Policy are considered violations of the Student Discipline Code and may result in disciplinary action as specified therein.

The District periodically may make determinations on whether other incidental non-educational uses of the Network are consistent with this Agreement. Uses that interfere with normal District business or educational activities are prohibited and may be cause for disciplinary action at the discretion of the District.

It is within the rights of the District to periodically modify the list of acceptable uses.

The District, in combination with the Information Technology Center (ITC) providing Internet access, will utilize filtering software or other technologies designed to restrict users from accessing visual depictions that are (1) obscene, (2) child pornography, or (3) harmful to minors, as these terms are defined and interpreted by the Children's Internet Protection Act and applicable state and federal laws.

As it is impossible to limit access to all materials that may be considered to be inappropriate, students are responsible for their use of the Network and are required to avoid sites that are inappropriate for the educational setting. Students are prohibited from taking any measures to override the filtering software. The District shall monitor students' online activities, through direct observation and/or technological means, to endeavor to ensure that users are not accessing such depictions or any other materials that are inappropriate for the educational setting.

I. Terms and Definitions:

1. The term computer or computer equipment includes: system units, displays, mice, keyboards, speakers, microphones, scanners, video projectors, video cameras, printers, hubs, switches, routers, patch panels, wiring, connectors, programs and any other piece of equipment or software which is part of the school's computer system.
2. The network is defined as all computers and other devices that are interconnected to the District local/wide area network and is the sole property of the Findlay City School District.

3. The Internet is defined as a collection of networks linking millions of computers and hundreds of millions of users all over the world.
4. Electronic Communication includes, but is not limited to, email, blogs, podcasts, discussion boards, web sites, video conferencing and virtual classrooms.
5. Portable electronic devices include, but are not limited to, laptop computers, personal digital assistants (PDAs), cellular telephones, recording and/or storage devices.
6. Web Page - A document designed for viewing in a web browser, typically written in hypertext markup language (HTML).

II. Acceptable Student Use:

1. Students may only access the district network and/or Internet by using their assigned network account. Use of another person's account/password is prohibited. Students may not allow other users to utilize their passwords.
2. Students may not intentionally seek or suggest to other students to seek information on, obtain copies of, or modify files, data or passwords belonging to other users, or misrepresent other users on the network.
3. Students may not upload, download, create or transmit confidential information, a computer virus, worm, Trojan horse, or other harmful components or corrupted data, or vandalize 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.
4. Students may not purposely engage in computer activities 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 email", use up limited Network capacity resources.
5. Students are encouraged to save and store their work in their server account, understanding that school staff may review computer files or messages that are created by the student. Material may be reviewed for grading and appropriate content. Additionally, files may be reviewed for any harassing or threatening material, and/or any vulgar or obscene content.
6. Students are not to modify or remove any identifying labels on computer equipment.
7. Students are permitted to use networked software and school-supplied software. Programs written by the student which are part of an assignment in a school's course of study may be run, as required, for that course of study's requirements, with teacher supervision.
8. Students may not install or delete programs on the school's computers. Students may not download programs from the Internet or any portable device and attempt to install onto District computers.
9. Students shall not remove, alter or copy Network software for their own personal use or for the use of others.
10. All electronic communication between students and teachers should take place through their district assigned accounts.
11. Students are asked to advise school staff when they observe any violation of the school's policy for the use of the school's computers.
12. Students are asked to advise their teacher when a computer malfunctions in any way.
13. Students may not use the District's computers or network to offer for sale any substance the possession or use of which is prohibited by law or the Student Discipline Code.
14. Students may not create, copy, view, transmit, download, upload, or seek, sexually explicit, obscene or pornographic materials.
15. Students may not create, copy, view, transmit, download, or upload 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 or the Student Discipline Code.

16. Students may not upload, download, copy, redistribute or republish copyrighted materials without permission from the owner of the copyright. Even if materials on the Network are not marked with the copyright symbol, students should assume that they are protected under copyright laws unless there is explicit permission on the materials to use them.
17. Students may not use web proxies to view, download or seek materials, files, information, software or other content that may be offensive, defamatory, misleading, infringing, or illegal, or to view or access content or information unrelated to the curriculum.
18. Students may not post or distribute inappropriate photos or media (pornography, dangerous, or hate-related media of any kind). This includes cyberbulllying 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 its 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.

Exceptions to any of the above rules are permitted only under direct teacher supervision. Violations of these rules may result in disciplinary action, including, but not limited to, termination of access to the school's computers, detention and/or suspension. Violations also may be referred to the appropriate legal authorities and/or other legal action may be pursued.

III. Server Storage

Each user is granted an equitable share of our storage resources. Requests for increased disk quota may be granted with a valid reason AND a staff sponsor. Such increases are temporary, lasting only for the duration of the project.

IV. Electronic Communication

E-mail and Instant Messaging are communication tools, which allow students to communicate one-to-one with people throughout the world. Students may be provided with individual e-mail or communication accounts under special circumstances, at the request and under the supervision of their teacher. Students may not attempt to establish outside web e-mail accounts through the School's network. 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:

1. 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 FLAMING, SCREAMING, demeaning or other inappropriate communications.
2. 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.
3. 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.
4. Sending e-mail attachments that are too large to be accommodated by the recipient's system.

5. Communications that violate any District Policy or the law.
6. All electronic communication across the District's network is a matter of public record and should never be considered private or secure.

V. Internet Safety

1. All 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 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.
2. 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. Students should never give out private or confidential information about themselves or others on the Internet.
3. Internet filtering software or other technology based protection systems may only be disabled by the IT department at the request of a principal or school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by students age 17 and older.

VI. Privacy

Network access is provided as a tool for your 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 and other content transmitted, received or stored in connection with this usage. All such information, content and files shall be, and remain, 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 insuring that users are using the system consistently with this policy.

VII. 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.

VIII. 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 tenure 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.

IX. 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 attorney's fees) of any kind suffered, directly or indirectly, by any student or parent/guardian arising out of the student's use of, or inability to use, the Network. Each student 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 student'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 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 Information Technology Center (ITC) providing Internet access and all of their administrators, teachers and staff harmless from any and all loss, costs, claims or damages (including attorney's 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.

Denial of Permission for Internet Access by Parent/Guardian

School Year _____

I have reviewed the Student Acceptable Use Policy – BOE Policy 9.27, which describes the terms of student access to interconnected computer systems, computer equipment, computer programs, the Internet, electronic mail and other new technologies within the Findlay City School District.

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;
- Will have access to interconnected computer systems, computer equipment, computer programs, electronic mail and other new technologies within the School District, other than Internet;
- Will be obligated to comply with all remaining terms of the Acceptable Use Policy (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 the parent/guardian and the undersigned student.

The Denial of Permission for Internet Access will be limited to the School Year requested above.

_____ _____
Name of Student (Print clearly) Grade

_____
Name(s) of Parent/Guardian

_____ _____
Signature of Parent/Guardian Date

_____ _____
Signature of Student Date

Adopted 4/23/01; Revised 8/25/03; Adopted 5/29/07; Adopted 7/19/10; Reviewed 6/18/2012