Book	Policy Manual
Section	7000 Property
Title	STUDENT ACCEPTABLE USE POLICY
Code	po7540.03
Status	Active
Adopted	October 6, 2011
Last Revised	May 16, 2016

7540.03 **- STUDENT ACCEPTABLE USE POLICY**

Students are encouraged to use the technology available in the Ottawa Hills Local School District. The District's technology is an important educational resource, which provides opportunities for collaboration and exchange of information; facilitates personal growth in the use of technology; and enhances information access, retrieval, evaluation, usage, and communication skills.

Session I of the Acceptable Use Policy was prepared to help students and parents/guardians understand relevant terminology. Section II contains the terms of the agreement and the agreement signature page. The agreement signature page must be completed and returned to the District's curriculum office.

Section I: Terminology

A. Acceptable Use Policy

   Our **Acceptable Use Policy** outlines the general guidelines and the acceptable uses of the technology available in the School District. This policy enables parents to give informed consent to use of District resources. In order for each student to have Internet access, there must be a signed **Acceptable Use Policy Agreement** on file (see Section II of this document).

B. The Internet

   The Internet is a network of networks used by educators, businesses, government, the military, organizations, students, and other individuals. In schools and libraries, the Internet can be used as a learning resource.

C. Data Acquisition Site/NWOCA

   The Northwest Ohio Computer Association (NWOCA) serves as the District's link to the Internet. Our direct connection goes through NWOCA and out to the Internet.

D. Account

   Each student and staff member will be provided a basic account on the Ottawa Hills network (internal). Each account will be given a level of access, maximum amount of disk space to be used, printing quotas, etc. Students with a signed **Acceptable Use Policy Agreement** on file will have additional access based upon the consent of the parent/guardian.

E. User
   A user is a student, staff member, or other person with a network account.

F. Password

A password enables users to access the network services. Each registered user will be issued an account. Students with a signed *Acceptable Use Policy Agreement* on file will be granted Internet access through this account. Like a house key, password should not be given to anyone. **Anything that happens on the network, under a specific individual's account and password, is that individual's responsibility.**

G. Shareware and Freeware

A shareware program is a copyrighted computer program that is made available free of charge on a trial basis. If the user likes the program and decides to use it, the user is expected to pay a fee to the author. A freeware program is a copyrighted program that has been made available without charge for public use.

H. Software Piracy

Software piracy is the unauthorized duplication of software and is a federal offense. Students are not to copy the District's software nor are they to load personal software on to the District's computers.

I. Technological Vandalism

Technological vandalism is the intentional damaging of technology (hardware and software) or posting of obscene, profane, insulting, discriminatory, or harassing remarks on computers, over the Internet, or on other technological devices. Examples of vandalism include altering the system and/or network configurations, attempting to bypass network security, intentionally spreading viruses, damaging equipment, or conducting illegal activities, to name a few. Students found vandalizing technology (hardware or software) will be dealt with according to the school's vandalism policy as it is established in the student handbooks. Students will lose network and Internet privileges and be responsible for all damages.

Statement of Purpose

Ottawa Hills Local Schools (hereafter referred to as District) is pleased to offer our students access to the World Wide Web and other electronic networks. Students are encouraged to use the technology available in the District. The District's technology is an important educational resource, which provides opportunities for collaboration and exchange of information; facilitates personal growth in the use of technology; and enhances information access, retrieval, evaluation, usage, and communication skills. However, it is important to remember that access is a privilege, not a right, and carries with it responsibilities for all involved.

This *Acceptable Use and Internet Safety Policy* is an agreement between the student, parent/guardian, and the District. The intent of this document is to ensure that parents are knowledgeable about and that students will comply with the *Acceptable Use and Internet Safety Policy* approved by the District. The agreement signature page must be completed and returned to the
Technology office.

Terms of Agreement

Personal Responsibility, Use and Acceptance

In exchange for the use of the District computers and other hardware, Internet access, email, electronic subscriptions/research/productivity resources, and internal electronic resources (hereafter referred to as the Network), we (parents/students) understand and agree to the following items (as signified by signing the attached agreement). Students who use or otherwise access the District's Network via wireless or hardwired connection (hereafter referred to as Users) are responsible for their behavior on the Network just as they are in a classroom, school hallway, or other School District property. The User consents to the terms of this Policy whenever he or she accesses the Network. The District reserves the right to remove files, limit or deny access, and/or refer a student for other school disciplinary action and/or, if necessary, criminal prosecution as a result of any improper use, determined by the District, and is not limited by the examples of misuse given in this Policy.

Infractions to the Acceptable Use and Internet Safety Policy will be in accordance to the school discipline policies. All school rules, regulations, and consequences specified in the student handbooks regarding violations such as use of profanity, harassment, theft, misuse, vandalism, etc. will apply. Students will be liable for any damages caused by misuse of access privileges.

The use of the Network is a privilege not a right. This privilege may be revoked by the District at any time and for any reason. The use of District and/or Network resources are for the following purposes (in order of priority):

A. support of the academic program

B. telecommunications for academic purposes

C. general information and research

The District reserves all rights to any materials stored in files which are generally accessible to others and will remove any material which the District, at its sole discretion, believes may be unlawful, obscene, pornographic, abusive, or otherwise objectionable.

Students will not use their District-approved computer account/access to obtain, view, download, or otherwise gain access to such materials.

All information services and features contained on District and/or Network resources are intended for the private use of its registered Users. Any use of these resources for commercial-for-profit uses, intrusion on other Users' privacy, or other unauthorized purposes (i.e., advertisements, political lobbying), in any form, is expressly forbidden.

No personal equipment is permitted to be connected to the Ottawa Hills Private Network. This includes, but is not limited to, personal computers or tablets, handhelds, phones, gaming consoles, etc. In addition no equipment shall be connected to the Ottawa Hills Private Network that is expressly prohibited by the Northwest Ohio Computer Association (NWOCA). Said equipment includes, but is not limited to, routers, modems, wireless networking equipment, and managed switches. Under no circumstances should District owned technology be moved from one location to another without permission of the District Technology Director.

The District and/or Network are intended for the exclusive use by registered Users. Anonymous use is not permitted and access (including passwords) may not be shared or transferred. Any improper use of your account, even if you are not the User, is your responsibility. The student is responsible for the use of his/her account/password and/or access privilege. Any problems that arise from the use of a student's account are the responsibility of the account holder. Students are responsible for logging out of their individual account at the end of each use. Use of an account by someone other than the registered account holder is forbidden and may be grounds for loss of access privileges and for other school disciplinary actions. Users must report any misuse of the Network, including security/password breaches, to the District Technology Director or building administrator.

Any misuse of District technology, User accounts, or Network resources will result in suspension of access privileges and/or other disciplinary action determined by the District. Misuse shall include, but not be limited to:

A. intentionally seeking information on, obtaining copies of, or modifying files, other data, or passwords belonging to other Users; logging on to other Users' accounts (for any reason)

B. allowing anyone other than the account holder to use an account, sharing your password with anyone or logging other Users onto your account

C. impersonating other Users on the Network through any electronic communication

D. interfering with others' use of the Network; disrespecting other Users' rights to privacy

E. accessing or attempting to access information in areas students do not have access to

F. use of anonymous proxies or any other attempts to circumvent content filtering is strictly prohibited and is a direct violation of this agreement

G. malicious use of the Network through hate mail, harassment, profanity, vulgar or threatening statements, cyber bullying, or discriminatory remarks

H. extensive use for noncurriculum-related communication

I. using District provided electronic communications for expression of opinions, as a public forum of any kind, or to support private or public causes or external organizations

J. engaging in commercial transactions. Students may not use the school Network to sell or buy anything over the Internet.

K. engaging in or promoting any other activity deemed illegal by local, State or Federal law

L. violating copyright law, which includes but is not limited to the storage or illegal use of copyrighted software, text, audio and video files as well as video games

M. downloading, installing, or using any software or other tools that are not District owned or approved to be used on the computer or Network. No third party software will be installed or used without the consent of the Technology Director.

N. using the intellectual property of others without permission and/or without citing the author

O. disrupting the operation of the Network through abuse or alteration of any District owned hardware, software, or Network resources

P. attempting to hack into any District owned hardware, software, or Network resources

Q. vandalizing District owned hardware, software, or Network resources

R. **USE OF OUTSIDE SERVICES**: All email, document storage, blogs, social networking, or any and all other online services must be approved by the School District on its Network. The use of other providers of such functionality or storage (such as Facebook, Twitter, personal Google account, personal email accounts) through the District's Network is prohibited. Permission to access these services may be granted on a limited basis by the District Technology Director. A student must obtain permission prior to access.

S. neglecting to follow guidelines of Web 2.0 tools (outlined in separate section below.)

T. using technology and Web 2.0 tools to facilitate academic dishonesty

The student will diligently delete documents on a regular basis from his/her District issued Network account to avoid excessive use of disk space. The student will refrain from saving noncurriculum related files onto their District issued Network accounts such as personal photos and music. The Technology Director has the authority to periodically purge the system.

The District reserves the right to impose time limits, access limits, and disk and printer quotas. Academic pursuits take priority over all other activities.

The District reserves the right to log computer use and to monitor fileserver space utilization by Users. The District reserves the right to remove a User account from the Network to prevent further unauthorized activity.

The District and/or Technology Director will periodically make determinations on whether specific uses of District technology are consistent with the acceptable-use practice.

Use of Web 2.0 Tools

Online communication is critical to our students learning 21st Century Skills and tools such as blogging, email, online/cloud computing, and podcasting offer an authentic, real-world vehicle for student expression. The primary responsibility to students is their safety.

Hence, expectations for classroom projects or other Web interactive activities, such as blogging, email, online/cloud computing, and podcasting must follow all established Internet safety guidelines.

A. The use of blogs, email, online/cloud documents, podcasts or other Web 2.0 tools is considered an extension of the classroom. Therefore, any speech that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, email, online/cloud documents, podcasts, or other Web 2.0 tools. This includes, but is not limited to, cyber bullying, profanity, racist, sexist or discriminatory remarks.

B. Students using blogs, email, online/cloud documents, podcasts or other Web 2.0 tools are expected to act safely by keeping ALL personal information out of their posts.

C. A student should NEVER post personal information on the web (including, but not limited to, last names, personal details including address or phone numbers, or photographs). Do not, under any circumstances, agree to meet someone you have met over the Internet.

D. Comments made on blogs, email, online/cloud documents, podcasts will be monitored and - if they are inappropriate – will be deleted and disciplinary action may be taken.

E. Never link to web sites from your blog or blog comment without reading the entire article to make sure it is appropriate for a school setting.

F. Students using such tools agree to not share their User name or password with anyone besides their teachers and parents and treat blog spaces as classroom spaces. Speech that is inappropriate for class is also inappropriate for a blog.

G. Students who do not abide by these terms and conditions may lose their opportunity to take part in the project and/or be subject to consequences appropriate to misuse.

Internet Safety

A. Parents and Users - Despite every effort for supervision and filtering, all Users and their parents/guardians are advised that access to the electronic Network may include the potential for access to materials inappropriate for school-aged students. Every User must take responsibility for his or her use of the Network and Internet and avoid these sites.

B. Personal Safety - In using the Network and Internet, Users should not reveal personal information such as home address or telephone number. Users should never arrange a face-to-face meeting with someone "met" on the Internet without a parent's permission.

C. Confidentiality of Student Information - Users are responsible for maintaining the security of their data and other personally identifiable information. Users should never give out private or confidential information about themselves or others on the Internet. Users are responsible for the data that is downloaded from the Network to their computer screen, transmitted by email, stored on a flash drive, portable device or laptop, copied by handwriting or by any or all other devices, forms of storage or methods.

D. Active Restriction Measure - The District will utilize filtering software or other technologies to prevent students from accessing visual depictions that are (1) obscene, (2) pornographic, or (3) harmful to minors. The use of anonymous proxies or any other attempts to circumvent the content filter is strictly prohibited and will be considered a violation of this policy. The school will also monitor the online activities of students, through direct observation and/or technological means.

E. The District will provide age-appropriate training for Users who access the Internet through the District Network. Following receipt of this training, the User will acknowledge that he/she received the training, understood it, and will follow the provisions of the policy herein. The training provided will be designed to promote the District commitment to:

1. The standards and acceptable use of Internet services as set forth herein;

2. Users safety with regard to:

    a. safety on the Internet;

    b. appropriate behavior while on online, on social networking websites, and in chat rooms; and

    c. cyber bullying awareness and response.

3. Compliance with the E-rate requirements of the Children's Internet Protection Act ("CIPA").

Waiver of Privacy

The District reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer Network, Internet access, and any use of District provided equipment and services. All such data and transmissions shall be and remain the property of the District and no User shall have any expectation of privacy regarding such materials.

System Security and Integrity

The District has defined these guidelines to help students and to insure an understanding of appropriate use and expectations. The District reserves the right to suspend operations of the Network, in whole or in part, at any time for reasons of maintaining data security and integrity or any other lawful reason. The District reserves the right to block or filter any web sites, email addresses, servers or Internet domains which it, in its sole judgment, has determined to present a risk of exposing students or employees to sexually explicit or otherwise inappropriate content, or which exposes the system to undue risk of compromise from the standpoint of security or functionality. Staff members will exercise reasonable care in supervising student use; however, the District and its personnel are not responsible for student exposure to objectionable or inaccurate content or for the unauthorized activities of a User.

No Warranties Created

The District and/or Technology Director do not warrant that the functions of the system will meet any specific requirements the User may have or that it will be error free or uninterrupted; nor shall it be liable for any direct or indirect, incidental, or

consequential damages (including lost data, information, or time) sustained or incurred in the connection with the use, operation, or inability to use the system. Students are to report any problems to the teacher, who shall notify the Technology Director.

In consideration for the privileges of using the District Network and/or research resources, and in consideration for having access to the information contained on or by the Network, we hereby release the District, Network, the data acquisition site, and their operators and administrators from any and all claims of any nature arising from the use or inability to use the District, Network, and/or research resources.

We (student and parent/guardian) agree, by signing the Acceptable Use and Internet Safety Policy Agreement, to abide by such rules and regulations of system usage as well as by any changes deemed necessary by the District Technology Coordinator. These rules and changes will be available in hard copy form in the Technology office and from the District Technology Director.

Student's Name (please pri

_____   _____
Last   First

OTTAWA HILLS LOCAL SCHOOLS

ACCEPTABLE USE AND INTERNET SAFETY POLICY AGREEMENT

This agreement is entered into this _____ day of _____ , 20 __ between
_____(student),

_____(parent/guardian), and the Ottawa Hills Local Schools.

We (parent/guardian and student) have read the ***Ottawa Hills Local Schools Acceptable Use and Internet Safety Policy*** and are willing to abide by said rules and regulations of system usage as well as any changes deemed necessary by the District Technology Director. These rules and changes will be available in the Technology office, from the District Technology Director, from the building principals, and on our district website

COMPLETE PART I, OR PART II, BUT NOT BOTH

PART I – CONSENT OF DISTRICT NETWORK AND INTERNET USE

By signing below, I approve access to the District Network, including individual student access to the internet.

_____   _____
Signature of Student (for grades 3-12 only)   Grade Level

_____   _____
Signature of Parent/Guardian (for grades K-12)   Date

PART II – PARTIAL CONSENT OF DISTRICT NETWORK AND INTERNET USE

By signing below I approve access to the District Network and to the Internet according to the indication below. Please check ONLY the one box that applies. One cannot have Internet access without access to our District Network.

☐   I do approve access to District Network but DO NOT approve access to the Internet.

☐   I DO NOT approve access to the District Network and DO NOT approve access to the Internet.

_____   _____
Signature of Student (for grades 3-12 only)   Grade Level

_____   _____
Signature of Parent/Guardian (for grades K-12)   Date

Parent/guardian signatures (for all grades) and student signatures (for grades 3-12 only) are required for use of these services and indicate that the parent/guardian and student have read and agree to the Ottawa Hills Local Schools Acceptable Use and Internet Safety Policy.

This agreement must be signed every school year and upon enrollment to the Ottawa Hills Local School District.

Note: Please return this signed agreement on schedule pickup day (grades 7-12) and on the first day of school (grades K-6).

Revised 8/2/12