Eastern School District
Computer Network and Internet Use Policy 2016-2017

Complete Board Acceptable Use Policy . . . . . 2 – 7

Rules Summary 8

Signature Page (for all students PS-12) 9

Addendum for "Bring Your Own Technology", Grades 4-12 ONLY.....10
(Requires separate signature page)

Eastern School District
Computer Network and Internet Use Policy

This document constitutes the School District's Computer Network and Internet Acceptable Use Policy, (Policy) and applies to all persons who use or otherwise access the District Network and/or Internet, whether with District or personal equipment or whether on-site or by wireless or other remote access ("Users"). In order for a student to be have access to a school computer, computer network, and the Internet, a parent and the student must sign and return the attached consent form.

1. Definitions. For purposes of this Policy,

- the term "Network" shall mean the District's group of interconnected computers and peripherals, via cable or wireless, all other District software and hardware resources including all Web-based material and all Web hosting, all data, databases and storage media, all standalone, portable and/or borrowed devices, and all provided connectivity between and among Users and from Users to the global Internet, including any and all Instructional Technology Centers or other third-parties providing connectivity and other services, and any and all identifiers, accounts, rights, permissions, and current or future hardware, software, or connectivity owned or managed by the District to which access is provided to Users. Personal electronic devices are considered to be part of the "Network" when they are brought to, and used in the buildings, and are subject to all terms of this Policy even when the User is not attempting to connect to another computer or to the Internet.

- the term "Use" of the Network shall mean any and all actions of a User which create traffic on the Network, including traces or remnants of traffic that pass through District equipment, wiring, wireless networks, or storage devices regardless of any other factor such as passage of time, user deletion, transit of the Network without storage or origination and/or storage on personal equipment.

2. Purpose and Use: The School District provides users access to its Network and Internet for educational purposes only. Access to system computers and the Network is a privilege, not a right, and carries with it responsibilities for all involved. The District reserves the right to withdraw access at any time for cause. The District reserves the right to determine what constitutes an improper use of system computers or the Network, and is not limited by the examples of misuse given in this Policy. Users may violate this Policy by evading or circumventing the provisions of the Policy, alone or with others. If Users have any doubt about their obligations under this Policy, including whether a certain activity is permitted, they must consult with the District Technology Director to be informed whether or not a use is appropriate.

3. Users Bound by Policy: The User consents to the terms of this Policy whenever he or she accesses the Network, whether with district-provided technology or personal devices. Users of the Network are bound to the terms of this Policy regardless of whether or not a copy was received and/or signed for by the User. Upon reviewing this policy, signing, and returning the agreement, each student will be granted limited use of the District's computer network and Internet. A copy of this policy shall be made available upon request and will be posted on the District website. Any parent or guardian of a student that is 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 District Technology Office. The signed form, when returned, is good for one year. Students will be asked to submit a new signed form at the beginning of each school year

4. Personal Responsibility: Network and Internet access is provided as a tool to support the education of students. In order for the District to control student access to electronic communications, the Internet and to continue to make its computer network available, all users must take responsibility for educationally appropriate and lawful use of this access. Students must understand that one student's misuse of electronic communication devices; internet access or the network may jeopardize the ability of all students to enjoy such access. While the District's teachers and other staff will make reasonable efforts to supervise student use, they must have student cooperation in exercising and promoting responsible use. Users are responsible for their behavior on the Network just as they are in a classroom, school hallway, or other School District property. Each User is responsible for reading and abiding by this Policy and any and all future amendments, which will be made readily available in both electronic and printed form. Anonymous use is not permitted and access to the network (including passwords) is not to be shared or transferred. If a User suspects that a password is not secure, he or she must inform a teacher, building administrator, or Technology Director immediately. Any improper use of your account, even if you are not the User, is your responsibility.

5. Reporting Misuse of the Network: Users must report any misuse of the Network to a teacher, building administrator, or Technology Director. “Misuse” means any apparent violation of this Policy or other use which has the intent or effect of harming another person or another person’s property.

6. Violating Policy with Personal Equipment: The use of personal equipment and/or personal Internet access to violate this Policy or to assist another to violate the Policy is prohibited. For this policy, these devices shall be defined as personally owned devices that can be connected to voice or data network. Current examples include, but are not limited to, cellular phones, SmartPhones, netbooks, notebooks, iPods, iPads, tablet devices, etc. The use of any of these devices on the Eastern network requires special permission from a building administrator and the IT Department. Exceeding permission (such as abusing access) is a violation of this Policy. Using private equipment to divert student time and/or attention from scheduled educational activities, or to divert paid work time from its proper purpose, is always strictly prohibited. Personal equipment used to violate this Policy on school property is subject to search related to the violation and seizure.

7. Discipline for Violation of Policy: Violations of each of the provisions of this Policy are considered violations of the Student Code of Conduct, and each violation is a separate infraction. Violations may result in disciplinary action for students up to and including suspension or expulsion and/or referral to law enforcement based on the severity of the offense. The District reserves the right to seek reimbursement of expenses and/or damages arising from violations of these policies.

8. Waiver of Privacy: By accepting Network access, Users waive any and all rights of privacy in connection with their communications and files on the Network or communications achieved through the use of District equipment or software. Electronic mail (e-mail) and other forms of electronic communication (including instant messaging of all forms and SMS messages originating from email) are not guaranteed to be private. The District uses a CIPA-compliant Internet logging and tracking system, which logs all Internet traffic. The District owns all data in the system. The wireless access provided for personal device usage also requires user authentication and filters and keeps a log of all Internet traffic. Although the District respects the natural desire of all persons for privacy and will attempt to preserve this privacy whenever possible, the operational and security needs of the District's computer network and messaging systems require that full access be available at all times. The District therefore reserves the right to access and inspect any computer, device, or electronic media within its systems and any data, information or messages which may be contained therein. Systems managers have access to all messages for purposes of monitoring system functions, maintaining system efficiency, and enforcing computer/network use policies and regulations, District policies, and state and federal laws. Illegal activities or suspected illegal activities may be reported to the authorities.

9. Security and Integrity: Staff members are responsible for maintaining security of student information and other personally identifiable data that they access, even if they access such data accidentally or without permission, and for upholding FERPA (20 U.S.C. § 1232g), the student confidentiality law (Ohio Revised Code Section 3319.321), the Ohio Privacy Act (Chapter 1347 of the Ohio Revised Code), and any other applicable privacy policies and regulations. Users are responsible whether such data is downloaded d from the Network to their computer screen, transmitted by e-mail, stored on a flash drive, portable device or laptop, copied by handwriting or by any or all other devices, forms of storage or methods. Negligence with respect to protecting the confidentiality of such data will be considered a violation of this Policy whether or not such negligence results in identity theft or other harm.

10. District-Owned Equipment: Desktop computers, laptops, portable devices, and other equipment belonging to the District are your responsibility. Any misuse, failure, damage or loss involving such equipment must be reported to a teacher, building administrator or Technology Director immediately. Periodic maintenance on laptops and other hardware is required. It is your responsibility to make such equipment timely available for maintenance at the request of the IT Department. You may be held financially responsible for the expense of any equipment repair or replacement, if damage was the result of misuse, vandalism or negligence.

11. Unacceptable Uses of the Network: All Users must use the Network in an appropriate and responsible way, whether their specific actions are described in this Policy or not. Examples of unacceptable uses include, but are not limited to, the following

- OFFENSIVE OR HARRASSING ACTS: Creating, copying, viewing, transmitting, downloading, uploading or seeking sexually explicit, obscene, or pornographic materials. Using language inappropriate to the school environment, including swearing, vulgarities or language that is suggestive, obscene, profane, abusive, belligerent, harassing, defamatory or threatening. Making, distributing or redistributing images, 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. Engaging in harassment, stalking, or other repetitive unwanted communication or using the Internet in support of such activities.

- CYBERBULLYING: Using the network via personal or district-owned devices to "Harass or Bully, as defined in the District Anti-Bullying policy" is prohibited. Violators shall be subject to the disciplinary actions contained in both the District's Acceptable Use and/or Anti-Bullying Policies.

- VIOLATIONS OF PRIVACY: Using an account that is not yours, allowing another user to use your account, or providing your account information to someone else. You are responsible for any and all activity that occurs under your account. Unauthorized copying, modifying, intruding, or attempts to copy, modify or intrude, into the folders, files, data, work, networks, passwords or computers of others, or intercepting communications intended for others. Copying, downloading, uploading, or transmitting student or School District confidential information.

- CREATING TECHNICAL PROBLEMS: Users may not knowingly attempt to:
  - Cause technical difficulties for the network, other users or impede efficient use of the internet
  - Bypass district internet filtering or use alternate programming to access a site that would otherwise be blocked
  - Attempt to "hack" into other accounts or restricted information
  - Upload, download, create, or transmit a computer virus, worm, Trojan horse, or other harmful component or corrupted data
  - Attempt to hack, alter, harm, destroy or interfere with the normal operation of software, hardware, data, other District Network resources, or using the District Network or to do any of the same acts on the Internet or outside Networks
  - Download, save, and/or transmit data files large enough to impede the normal functioning of the computer or the Network (such as many music, video, image, or software files) unless given permission by the System Administrator
  - Move, "repair", reconfigure, reprogram, modify, or attach any external devices to Network equipment, computers or systems without the permission of the System Administrator
  - Remove, alter, or copy District software for personal use or for the use of others

- USE OF OUTSIDE SERVICES: All e-mail, document storage, blogs or any and all other services must be provided by the School District on its Network. Staff will have access to outside e-mail systems to be used for personal e-mail, subject to the loss of privacy rights as stated in this Policy All emails pertaining to district, school, or class business must be transmitted through the district email system. The district has an established relationship with Google and has its own Google Education Enterprise domain for hosted storage services. Students and staff may use this resource for outside storage.

- VIOLATING LAW: Actions that violate state or federal law or encourage others to do so. Offering for sale or use, soliciting the purchase or provision of, or advocating the use of any substance that the possession or use of is prohibited by law or District Policy. Seeking information for the purpose of creating an explosive device or biohazard, or communicating or seeking materials in furtherance of criminal activities, terrorism, or other threatening acts.

- VIOLATING COPYRIGHT: Uploading, downloading, copying, redistributing or republishing copyrighted materials without permission from the owner of the copyright. Users should assume that materials are protected under copyright unless there is explicit permission for use.

- PERSONAL USE:
  - Students are not permitted to make any commercial transaction using the school network. Personal shopping, buying or selling items, soliciting or advertising the sale of any goods or services, or engaging in or supporting any kind of business or other profit-making activity is not permitted.
  - Interacting with personal web sites or other social networking sites or tools that are not part of an educational or work project, receiving or posting messages to web sites or other social networking or blog sites not part of an educational or work project is not permitted. Facebook, MySpace and other social networking sites are not permitted for students.
  - Participating in any type of gaming activity, engaging in social or hobby activities, or general recreational web browsing if such browsing occurs during instructional time or designated work time.

- POLITICAL USE: Creating, transmitting or downloading any materials that support or oppose the nomination or election of a candidate for public office or the passage of a levy or a bond issue. Soliciting political contributions through the Network or conducting any type of official campaign business.

- GENERAL MISCONDUCT: Using the Network in a manner inconsistent with the expectations of the Eastern Local Schools for the conduct of students and employees in the school environment. Uses that improperly associate the School District with Users' personal activities or to activities that injure the District's reputation. Uses that mislead others or violate the standards of academic or personal integrity, including but not limited to plagiarism, disseminating untrue information about individuals or groups, or using another's password or some other user identifier. Downloading or installing any software on District computers. Students are not to download executable files, games, movie files, music files or picture files unless directly related to coursework. Students must receive permission to do this, even if downloads are directly related to coursework.

12. Specific Limits on Communication over the District Network:
- Expressing Opinion: The Network has been created at public expense and exists for purposes relating to education and administration. It does not exist to serve as a personal blog for the expression of opinions or as a public forum of any kind. It is not the intention of the District to allow the public, staff, or students to use the Network, including the web hosting or linking ability, for purposes of expressions of private opinions, or to support private or public causes or external organizations.

- Netiquette: In all electronic communications, users must abide by the rules of network etiquette, These include
  1. Be polite, use appropriate language, no vulgar, suggestive, obscene, or threatening language
  2. Don't communicate in a manner that others might find offensive
  3. Don't assume that the sender of an email is giving permission for you to forward or redistribute the message sent to you. Make sure you have permission to forward the email of another.
  4. Be considerate when sending attachments. Be sure that the file size is not too large for the recipient's email system.

- Large Group Mailings: The sending of messages to more persons than is necessary for educational or school business purposes is a misuse of system resources and user time. Large group mailings, such as "all district" or "all building" are reserved for administrative or business use, subject to any exceptions which may be developed by the Administration or the System Administrator. Student users may not send e-mails to more than ten (10) recipients in a single message, subject to exceptions developed by the Administration or the System Administrator. The System Administrator may also develop specific limitations on the use of graphics, the size, number, and type of attachments, and the overall size of e-mail messages sent on the system. The use of multiple messages, non-system addresses, or other techniques to circumvent these limitations is strictly prohibited.

- Personal E-mail: Limited personal use of District e-mail by employees to communicate with family, friends, and colleagues who are willing recipients is permitted as a personal convenience, but must not impact paid work time and is subject to all of the provisions of this Policy. Misuse of the privilege is prohibited, and includes but is not limited to excessive volume, frequency, inappropriate content, mailing to unwilling addressees, or uses that may bring the District into disrepute. Violations will be determined in the sole discretion of the Superintendent.

13. Use of New Web Tools: As the Internet continues to develop, new and innovative web tools are created. Many times these resources are referred to as Web 2.0 and these sites have great potential in the educational environment, offering students the opportunity to develop 21st Century Skills. These tools include blogging, podcasting, glogging, social bookmarking, wikis, to name just a few. Many of these sites require students to create their own individual account in order to use them and most either publicly or privately publish the students' works to the web. Teachers will incorporate these tools as appropriate into their curriculum. Therefore, students are reminded:

- The use of Web 2.0 tools is considered an extension of the classroom. Appropriate online behavior and language is required.
- Act safely; do not provide any personal information.
- All content posted onto a Web 2.0 site for school work, must follow the guidelines in this policy.
- Never include a link to another site in any school project, unless you have thoroughly investigated the link site and determined its authenticity and its validity.
- Do not share your username and password to any Web 2.0 site with anyone else.

14. System Security and Integrity: 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, e-mail 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.

15. No Warranties Created: By accepting access to the Network, you understand and agree that the School District, any involved Information Technology Centers, and any third-party vendors make no warranties of any kind, either express or implied, in connection with provision of access to or the use of the Network. They shall not be responsible for any claims, losses, damages or costs (including attorneys' fees) of any kind suffered, directly or indirectly, by any student or employee arising out of that User's use of and/or inability to use the Network. They shall not be responsible for any loss or deletion of data. They are not responsible for the accuracy of information obtained through electronic information resources.

16. CIPA Internet Safety and Instruction: All users should be advised that access to the Internet may include the potential for access to materials that are inappropriate for school-aged children. Every user must take responsibility for his or her use of the network and Internet and stay away from these types of sites. The District provides web filtering which blocks known harmful or inappropriate sites, but no solution is fool-proof. Teachers monitor students closely when they are on the Internet. Students in grades K-8 will participate regularly in teacher-led discussions of internet safety and cyberbullying using a variety of locally selected, grade level appropriate " internet safety" educational resources. Students in grades K—9 will participate in an Internet Safety curriculum each year that addresses Internet Safety, Appropriate Online Behavior, and Cyberbullying as required for E-Rate participation. Students in grades 10-12 will be reminded of the principles of internet safety, appropriate online behavior and cyberbullying on an ongoing basis, through bulletin boards, periodic educational email messages and announcements posted on the District websites, and in Language Arts and Social Studies courses. An Internet Safety Curriculum will be used, with resources from cybersmartcurriculum.org, www.isafe.org, www.learning.com, netsmartz.org and commonsense.org.

17. Publishing on the District websites: The District has a World Wide Web site on the Internet at ep.k12.oh.us This site is used for publishing district information, announcements, documents, curriculum resources and school news. As part of the overall curriculum and our own District information system, school news, awards, accomplishments, student projects and athletic information are published on our website. The kinds of student projects that may be published include, but are not limited to: creative writing, artwork, slide presentations, multimedia projects, reports, and web projects. News and athletic items might include pictures and information. The classroom teachers, website faculty advisors, student web teams and district administrators reserve the right to determine what kinds of work and information will be published. Parents have the right to refuse such information be published and must contact the Technology Office for the appropriate opt-out form. Eastern will publish information that the Board of Education has adopted as "directory" information and will follow these guidelines.

- A student's work may be identified by school, teacher or curriculum, and grade level
- If names are used at all, students' first names only will be used, or first initial, last name
- No personal contact information will be published

Legal Ref.: Ohio Rev. Code 3313.20, 3313.47, 3319.321
Children's Internet Protection Act of 2000, 47 USC § 254 (h), (l)
Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g
Revised: _7_ /_25_ / 2011_

Guidelines for the Eastern School Network Acceptable Use Policy

The Eastern School District provides access to a variety of electronic resources for use by students and teachers. The network is comprised of computers, printers, scanners and other electronic devices running instructional and productivity software and providing access to the internet.

Students and their parents are asked to carefully read and follow the terms of the District's Acceptable Use Policy that governs access and use to the network. Each year students (under age 18) must have a parent sign a copy of the Acceptable Use Contract acknowledging their willingness to comply the Policy.

In summary the contract contains:

Acceptance of personal responsibility for educationally appropriate use of the network.

Agreement to not share passwords or account information or use another's account.

Agreement to not misuse district equipment or the network in a way that negatively impacts network performance, physically damages equipment or alters software in ways that make it less useful.

Acknowledgment that information contained on the network and its devices are the property of the Eastern Local School District.

Acknowledgment that the network, and all devices are to be used in support of the educational purposes of the district.

Acknowledgment that all policies and restrictions apply equally to personal devices as well as district-provided devices

Agreement not to conduct any business or political activities via the network

Agreement not to violate copyright laws by downloading or redistributing copyrighted materials without the owner's permission

Agreement not to conduct any illegal activities on the network

Agreement to not use the Network in a manner inconsistent with the expectations of the Eastern Local Schools for the conduct of students and employees in the school environment

Agreement to not use the network to express personal opinions, and to be polite, not to be offensive, not to forward emails without the sender's permission and to be considerate when sending email attachments.

Acknowledgement of the District's role in maintaining security of the network, filtering internet content, logging internet traffic, and otherwise taking actions to maintain network safety and security.

Acknowledgment of the safety risks involved in accessing the internet and of the parent's role in advising their child in the safe use of the internet.

Agreement not to participate in any cyberbullying or hate mail activities.

Agreement not to access social networking sites that are not specifically dedicated to educational purposes.

Agreement to not attempt to bypass the District's internet filtering as required by CIPA (federal law).

Eastern School District
Computer Network and Internet Use Policy

Every student, regardless of age, must read and sign below

I have read, understand and agree to abide by the terms of the Computer Network and Internet Acceptable Use Policy. Should I commit any violation or in any way misuse my access to the District's computer network and the Internet, I understand and agree that my access privilege may be revoked and school disciplinary action may be taken against me.

(print clearly)

Last	First	MI	Grade

Signature	Date

Place an X in the correct blank: I am 18 or older _ I am under 18_

If I am signing this Agreement when I am under 18, I understand that when I turn 18, this Agreement will continue to be in full effect, and I will continue to abide by the Acceptable Use Policy.

PARENT OR GUARDIAN

I have received a copy of the Eastern Local School District's Acceptable Use Policy relating to student access to the District computer network and to the Internet and I grant permission for my child to have access to the Eastern Computer Network and Internet.

Parent/Guardian Signature	Date

Legal Ref.: Ohio Rev. Code 3313.20, 3313.47, 3319.321
Children's Internet Protection Act of 2000, 47 USC § 254 (h), (l)
Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g
Revised: /_ / 20_

PERSONAL ELECTRONIC DEVICES (Addendum)
Applies to High School and Middle School Students Only

In response to the growing need to provide more access to digital resources and the Internet, this policy was developed to allow high school students to bring their own devices. The Eastern Administration and Tech Department reserve the right to refuse any personal device it deems inappropriate or unacceptable to be brought into the school.

High School students are permitted to bring personal learning devices, such as laptop or tablet devices. These devices are to be used at the sole discretion of the classroom teacher and are to be used for research and work that supports educational purposes.

All users and personal devices must follow all the policies in the District Acceptable Use Policy. A signed AUP must be on file, in addition to this Personal Electronic Devices addendum. The following guidelines apply, and are specific to personal devices, in order to protect both the District network and the users.

Requirements:

The Eastern School District will not be held liable for any damage that may occur to the personal device as a result of connecting to the network or AC power source.

The Eastern School District will not be held liable for any physical damage, loss or theft of the device.

The District reserves the right to inspect any personal computing device to determine that the AUP is being followed.

Personal devices MUST be connected to the EPLS-BYOD Wi-Fi network when being used on school premises, NO

EXCEPTIONS.

Anti-virus software must be up-to-date and active. (Microsoft Security Essentials or AVAST are free anti-virus programs that could be used, if you do not have another package)

The use of personal electronic devices must comply with ALL policies and procedures in the District's full Acceptable Use Policy.

I have read and understand the guidelines in the Personal Electronic Devices addendum. I have read and signed the District Acceptable Use Policy. I understand that the District will not be responsible for any loss, theft, or damage to my device or the data it contains. The District will not backup data and files saved onto personal devices. I understand that inappropriate use will result in the revoking of my privilege to bring my own device to school and/or discipline under the District's Acceptable Use Policy.

I have read and understand the guidelines in the Personal Electronic Devices addendum. I have read and signed the District Acceptable Use Policy. I understand that the District will not be responsible for any loss, theft, or damage to my device or the data it contains. The District will not backup data and files saved onto personal devices. I understand that inappropriate use will result in the revoking of my privilege to bring my own device to school and/or discipline under the District's Acceptable Use Policy.

Student Signature _____ Date _____ Grade _____

Parent Signature _____ Date _____