

St. Clairsville School District

Computer Network and Internet Acceptable Use Policy For Staff

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 Network and/or Internet, whether with District or personal equipment or whether on-site or by wireless or other remote access ("Users").

1. **Definitions.** For purposes of this Policy,
 - the term "Network" shall mean the District's group of interconnected via cable and/or wireless computers and peripherals, 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. Individual system computers are considered to be part of the "Network" and are subject to the 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 is providing Users access to its Network to support and enhance the educational experience of students and to facilitate work duties of employees. Access to system computers and the Network is a privilege, not a right. The District reserves the right to withdraw access at any time for any lawful reason. 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 [Technology Coordinator & Superintendent] to be informed whether or not a use is appropriate.
3. **Users Bound by Policy in Accepting Access:** The User consents to the terms of this Policy whenever he or she accesses the Network. 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.

4. **Personal Responsibility:** 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 (including passwords) may not be shared or transferred. If a User suspects that a password is not secure, he or she must inform [Technology Coordinator] 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 “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 on our network to violate this Policy or to assist another to violate the Policy is prohibited. Exceeding permission (such as abusing access to unfiltered Internet connectivity) 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.
7. **Discipline for Violation of Policy:** Violations of each of the provisions of this Policy are considered violations of the Employee Conduct (of the contract of employment), and each violation is a separate infraction. law enforcement, or up to termination and referral to law enforcement for employees. The District reserves the right to seek reimbursement of expenses and/or damages arising from violations of these policies. Disciplinary action relating to employees is always subject to the provisions of any applicable collective bargaining agreement.
8. **Waiver of Privacy:** By accepting Network access, Users waive any and all rights of privacy in connection with their communications over 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 owns all data in the system for 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. **Confidentiality and Student Information:** Users 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 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 [Technology Coordinator]. You may be held financially responsible for the expense of any equipment repair or replacement.
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 without reporting immediately, 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.
 - **VIOLATIONS OF PRIVACY:** 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:** Knowingly performing actions that cause technical difficulties to the system, other users or the Internet. Attempting to bypass school Internet filters or to "hack" into other accounts or restricted information. Uploading, downloading, creating, or transmitting a computer virus, worm, Trojan horse, or other harmful component or corrupted data. Attempting 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. Downloading, saving, and/or transmitting 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. Moving, "repairing," reconfiguring, reprogramming, modifying, or attaching any external **(external storage devices are permitted)** devices to Network equipment, computers or systems without the permission of the System Administrator. Removing, altering, or copying District software for personal use or for the use of others.
 - **USE OF OUTSIDE SERVICES:** All e-mail, document storage, and all other services will be provided by the School District to the best of its ability on its Network. The use of other

providers of such functionality or storage (such as Google or Yahoo) through the Network is prohibited.

-
- **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:** 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 prohibited. 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, 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 is prohibited.
- **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 St.Clairsville Schools for the conduct of 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.

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, 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.

- **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 use, subject to any exceptions which may be 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. “Limited personal use” shall be defined as no more than ten (10) messages during any one day, with no attachments large enough impede the normal functioning of the computer or the Network, as determined by the System Administrator. Exceptions to this limitation may be permitted for personal emergencies and other extenuating circumstances.
- **Electronic Signatures:** Users shall not legally verify documents or use “electronic signatures” in any way unless they have been trained in an approved verification or signature system approved by the Administration. Users asked to legally verify or electronically sign documents should report the situation to [Technology Coordinator or Superintendent] .

13. 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 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.

14. 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 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.

15. Updates to Account Information: You must provide new or additional registration and account information when asked 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 [Technology Coordinator] or other person designated by the School District to receive this information.

16. Records Retention and Production: Users must comply with all District directions regarding the retention and management of e-mail or documents. The District retains the right to receive a copy of a record from an Employee User's private computer if for some reason it exists only on that computer.

[OPTIONAL:]

[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 in perpetuity without any ownership rights existing in the page creator(s). 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 for any reason or for no reason, in the sole judgment of [Superintendent or Technology Coordinator]. The School District does not intend to open web pages for the expression of opinion, and specifically does not intend for its web pages to be a public forum or limited public forum, staff, or citizens. Web pages exist solely in support of the School District functions and mission as determined by the Board.]

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____