

Ohio Hi-Point Career Center

Acceptable Use of Technology for Staff

Ohio Hi-Point Career Center ("OHPCC") provides its staff members access to appropriate usage of telephones, fax machines, computers and laptops, personal digital assistant devices (PDAs), e-mail, and the Internet ("electronic network") as deemed reasonable for the staff members' job duties. All staff members must take responsibility for appropriate and lawful use of this access.

PERSONAL RESPONSIBILITY

By accepting the account password and other information and accessing the electronic network the staff member agrees not only to follow the rules set forth in this policy, but also agrees to report any noted misuse of the electronic network to the Technology Coordinator. "Misuse" means any violation of this policy, or any other use not included in this policy, that may harm any individual or any individual's property. Staff assigned OHPCC-owned equipment to be taken home (laptops, PDAs, etc.) agree to accept personal responsibility for the care and safety of said equipment.

PURPOSE AND USE

Staff members are provided access to the electronic network for business and professional use. Although incidental personal use is permitted, such use is subject to all aspects of this regulation including the monitoring and access provisions. Personal use, however, should not be allowed to (1) impede the staff member's ability or the ability of others to get work done; or (2) adversely impact access to or the use of the system by others for business purposes. OHPCC shall be reimbursed by the staff member for all costs incurred by OHPCC as a result of personal use of any OHPCC-owned equipment or the electronic network.

GENERAL UNACCEPTABLE BEHAVIOR

Staff members are prohibited from engaging in any of the following activities while using any OHPCC owned equipment or the electronic network.

1. Sharing or revealing private login information with or to other staff members or students.
2. Everyone with access to the electronic network has their own private login. At no time shall a staff member allow anyone (including substitutes, visitors, and students) to use a computer while that staff member is logged in.
3. Posting information that, if acted upon, could cause damage or danger of disruption.
4. Revealing confidential information without proper authorization.
5. Engaging in personal attacks, including prejudicial or discriminatory attacks.
6. Engaging in threats to any person or entity.
7. Harassment or cyber-bullying, defined as persistently acting in a manner that causes distress or annoys another person. This activity also includes, but is not limited to, knowingly or recklessly posting or communicating false or defamatory information about a person or entity.
8. The use of criminal language or imagery, or language or imagery related to committing a crime, such as threats to the president, instructions on breaking into computer networks, child pornography, drug dealing, purchase of alcohol, gang or violence-related activities, threats to an individual, etc.
9. No electronic communication using school-owned equipment should contain profanity or vulgarities, or language that is suggestive or sexual, obscene, insulting, belligerent, defamatory, or racially or culturally insensitive.
10. Saving, accessing, or displaying electronic files on the electronic network, or any OHPCC-owned equipment which contain language or imagery that is profane or vulgar, suggestive, sexual, obscene, insulting, belligerent, defamatory, or racially or culturally insensitive (unless part of a classroom lesson).
11. Abuse of network resources such as sending chain letters or "spamming."

12. Attempting to access or "hack" into prohibited areas of the electronic network, including student information systems, business systems, or any other areas of the electronic network that the staff member had not been granted permission to access.
13. Knowingly spreading a computer virus.
14. Use of any aspect of the electronic network or any OHPCC-owned equipment to acquire, download, run, install, or store illegally acquired files, including, but not limited to, music, video, and video game files.
15. Use of any aspect of the electronic network or any OHPCC –owned equipment to acquire, download, run, install, or store software of any type that is used to illegally share files or access prohibited areas of the school's electronic network. This activity is illegal.
16. Installing purchased software on any OHPCC-owned equipment or the electronic network that is not owned by OHPCC without the express written permission of the Technology Coordinator.
17. Other uses or activities that violate the law, these regulations, or encourage others to violate the law or these regulations.
18. Attempting to repair district technology, or any action that voids manufacturer warranty.

PROPER USE OF E-MAIL ACCOUNT

Depending on the content of an email message, it may be a public record that needs to be maintained by the District in accordance with the Board of Education's Records Retention Policy and made available for inspection and/or copying upon request by a member of the public. The following procedures are established so that the District's e-mail and Internet capabilities are not compromised, and e-mail messages are maintained in accordance with Ohio law.

As a general rule, do not put anything in an e-mail that you would not put on School District letterhead.

1. Types of E-Mail Prohibited
 - a. Use of the District E-mail System to sell anything not related to OHPCC fundraising.
 - b. Use of the District E-mail System to solicit for personal gain, such as announcements about catalog or home parties, garage sales, auctions, etc.
 - c. Use of the District E-mail System for political campaigning or advertising, or for any other use of a political nature.
 - d. Excessive sending or forwarding of jokes, pictures, or similar fun forwards not of a business nature.
 - e. Any e-mail encompassing any of the restrictions as set forth in Section III above.
2. Email Archival
 - a. All e-mail messages sent through the OHPCC electronic network are archived for a period of time, ranging from short-term to permanent, in accordance with the Ohio Revised Code and the Board of Education's Record Retention Policy.
 - b. As a general rule, staff should consider all e-mail sent through the OHPCC electronic network to be public record.

PRIVACY

- a. Access to the electronic network is provided as a tool for business purposes. OHPCC reserves the right to monitor, inspect, copy, review, and store at any time and without prior notice any and all usage of the system and any and all materials, files, information, software, communications, and other content transmitted, received, or stored in connection with usage of the electronic network or OHPCC-owned equipment. All such information, content, or files shall be and remain the property of OHPCC and staff members should not have any expectation of privacy regarding those materials. The technology coordinator may review files and intercept communications for any reason,

for purposes of maintaining system integrity and ensuring the users are using the system consistent with applicable policies and regulations.

- b. The Ohio Hi-Point Career Center and/or its instructors may maintain one or more Facebook, Twitter, blog or similar Internet pages for educational and marketing purposes. The identity of those individuals who are accessing, affiliating or commenting on these pages may be visible to third parties not affiliated with the Ohio Hi-Point Career Center. The Ohio Hi-Point Career Center is not responsible for revealing the identity, profile or personal information of the user, including minor students, by third parties. It is the express responsibility of the user, or his/her parent or guardian, to protect the user's identity, profile and personal information.

PLAGIARISM AND COPYRIGHT INFRINGEMENT

Staff shall not, and shall not knowingly allow students to plagiarize works found on the Internet. Plagiarism is defined as taking the ideas or writings of others and presenting them as your own.

Files downloaded from the Internet may be considered copyrighted material and may be illegal to download. Music, movies, games, and other programs that are shared on Peer-to-Peer networks (Kazaa, LimeWire, BearShare, FrostWire, BitTorrent, etc.) should be considered illegal, and should not be downloaded. Having these programs (or other programs with a similar purpose) installed on any OHPCC-owned equipment is a direct violation of this policy in accordance with section (C)(15) above.

Fair Use doctrine allows for limited use of copyrighted material for instructional purposes, but excludes use of copyrighted material for projects where the student or district stands to benefit financially. Staff shall not knowingly permit students to violate the Fair Use or Copyright laws.

District policies on copyright will govern the use of material accessed and used through the OHPCC electronic network.

FAILURE TO FOLLOW REGULATION

Use of the electronic network and OHPCC-owned equipment is a privilege, not a right. Violation of the policies contained herein may result in loss of privileges to the electronic network and OHPCC-owned equipment, and may be subject to further discipline up to and including termination of employment.

WARRANTIES AND INDEMNIFICATION

The District makes no warranties of any kind, either, express or implied, in connection with its provision of access to or use of its systems. It shall not be responsible for any claims, losses, damages, or costs (including attorneys' fees) of any kind suffered, directly or indirectly, by any user arising out of the user's use of, or inability to use, the systems. By using the systems, the staff member is taking full responsibility for the use, and agrees to indemnify and hold harmless the District, its Board members, administrators, and staff, keep cost, claims, or damages (including attorneys' fees) resulting from access to and use of the systems through that staff member's account, whether that use is on a computer or on another's computer outside the network.

The Superintendent is responsible for determining what constitutes unauthorized or inappropriate use. The Superintendent may deny, revoke or suspend access to the Network/Internet to individuals who violate the District's Staff Network and Internet Acceptable Use and Safety Policy and related Guidelines and take such other disciplinary action as is appropriate pursuant to Board Policy.

2019/2020 OHIO HI-POINT CAREER CENTER

STAFF NETWORK AND INTERNET ACCEPTABLE USE AND SAFETY AGREEMENT

To access e-mail and/or the Internet at school, staff members must sign and return this form.

Use of the Internet is a privilege, not a right. The District's Internet connection is provided for business and educational purposes only. Unauthorized or inappropriate use will result in a cancellation of this privilege.

The District has implemented technology protection measures which block/filter Internet access to visual displays that are obscene, child pornography or harmful to minors. The District also monitors online activity of staff members in an effort to restrict access to child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors. The Superintendent or his/her designee may disable the technology protection measure to enable access for bona fide research or other lawful purposes.

Staff members accessing the Internet through the District's computers/network assume personal responsibility and liability, both civil and criminal, for unauthorized or inappropriate use of the Internet. The District reserves the right to monitor, review and inspect any directories, files and/or messages residing on or sent using the District's computers/networks. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

To the extent that proprietary rights in the design of a web site hosted on the District's servers would vest in a staff member upon creation, the staff member agrees to license the use of the web site by the District without further compensation.

Please complete the following information:

Staff Member's Full Name (please print): _____

I have read and agree to abide by the Staff Network and Internet Acceptable Use and Safety Policy and Guidelines. I understand that any violation of the terms and conditions set forth in the Policy is inappropriate and may constitute a criminal offense. As a user of the District's computers/network and the Internet, I agree to communicate over the Internet and the Network in an appropriate manner, honoring all relevant laws, restrictions and guidelines.

Staff Member's Signature: _____ Date: _____

The Superintendent is responsible for determining what is unauthorized or inappropriate use. The Superintendent may deny, revoke or suspend access to the Network/Internet to individuals who violate the District's Staff Network and Internet Acceptable Use and Safety Policy and related Guidelines and take such other disciplinary action as is appropriate pursuant to Board Policy.