

NETWORK ACCEPTABLE USE POLICY

The Hilliard City School District (“District”) recognizes that new technologies, such as use of computers, electronic mail (“e-mail”) and the Internet, open opportunities to new information and modes of communication. The use of e-mail and the Internet is a privilege. These technologies also alter instruction and student learning. The District supports access to appropriate resources by staff, volunteers and students (“users”) for educational purposes and other legitimate District business based upon the user’s legitimate needs. Due to the rapid change in technology, a user’s access and/or this Policy are subject to change at any time.

In exchange for the use of the Network resources, either on-site or by remote access, the user understands and agrees to the following:

1. **Privilege:** Access to the Network (i.e., e-mail and the Internet) is a privilege, not a right. Accordingly, access requires responsible and lawful use. The use of Network is a privilege which may be revoked by District at any time and for any reason. The District administrators and/or Network managers may perform the following actions for any legitimate reason, including but not limited to the purposes of maintaining system integrity and insuring that users are using the Network consistent with this Policy: 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, communication, and other content transmitted, received or stored in connection with this usage. The Network and all information, content, and files are the property of the District, and users should not have any expectation of privacy regarding those materials.
2. **Acceptable Use:** The Network shall be used primarily for educational and legitimate District business purposes. The District’s goal in providing this technology to users is to promote efficiency and excellence in the workplace and education, assist in the collaboration and exchange of information, facilitate personal growth in the use of technology and enhance information gathering and communications skills.
3. **Access:** Selected Network resources are intended only for use by their registered users. Users shall not have access to the Network until they have signed the Acceptable Use Agreement. Access is not transferable and may not be shared. Users shall not share their passwords or otherwise allow anyone to gain unauthorized access to the Network. A user is responsible for any violations of This Agreement committed by someone who, with the user’s express or implied permission, accessed the Network with the user’s password.
4. **Network Etiquette:** Use of the Network has great potential to enhance the productivity of the users. The Network, however, could also be abused. Users shall be held accountable for their use or misuse of the Network. All users are responsible for good behavior while using the Network, just as they are in a classroom, in a school hallway, or at any school-sponsored activity. Each user must abide by generally accepted rules of Network etiquette, which include but are not limited to:
 - a. Users shall not obtain copies of, or modify files, other data, or passwords belonging to other users without express authorization.

- b. Users shall not misrepresent themselves on the Network.
 - c. Users shall not use the Network in any way that would disrupt the operation of the network; intentionally abuse the software and/or hardware; or intentionally consume limited computer paper excessively or telephone resources, such as through spamming, creating or transmitting mass e-mails or chain letter, or extensively using the Network for noncurriculum-related communications or other purposes exceeding this Policy.
 - d. Users shall not create or transmit harassing, threatening, abusive, defamatory or vulgar messages or materials.
 - e. Except for educational or professional purposes, users shall not reveal any personal information beyond directory information about themselves, District employees, volunteers or students, including but not limited to a user's Network password(s) or social security numbers. Requests for information should be scrutinized by standards of public disclosure.
 - f. The confidentiality of any information stored in or created, received or sent over the e-mail system or through Internet access cannot be guaranteed.
 - g. Users shall not use the Network for any commercial activities, such as buying, advertising or selling goods or services, unless it is for legitimate District business, **EXCEPT any activity in the "Shopping Network" folder.**
 - h. Users shall not create, transmit or download any material that support or oppose the nomination or elections of a candidate for public office or the passage of a levy or bond issue, unless for legitimate classroom educational purposes, **EXCEPT any activity in the "HEA" or "OAPSE" folders.** Additionally, users shall not solicit political contributions through the Network from any person or entity, **EXCEPT any activity in the "HEA" or "OAPSE" folders.**
 - i. Users shall not create, transmit, download or copy any materials (a) that are in violation of District Polices or any federal, state or local laws, including but not limited to confidential information, copyrighted material, material protected by trade secrets, and any materials that would violate the District's harassment or discrimination policies; or (b) 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 pornographic, sexually explicit or obscene materials.
 - j. Users routinely shall delete outdated or unnecessary e-mails from their mailboxes.
5. **Web Sites:** Web sites created through the Network and/or linked to the District's web site for teachers, schools, or departments must relate specifically to those educational activities or programs. The District reserves the right to require that material and/or links to other sites found to be contrary to the District's interests be altered or removed. Any web pages created using the District's equipment or created as part of classroom or club assignment become the property of Hilliard City Schools. All web pages under this Policy, other than the official Hilliard City School District web site, must prominently display the following disclaimer:

This is not an official web site of the Hilliard City School District. The Hilliard City School District does not control and cannot guarantee the relevance, timeliness, or accuracy of the information on this web site. Any views or opinions expressed herein are solely those of the creators of this web site.

6. **Vandalism:** Vandalism is prohibited. Vandalism is 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 harm or destroy anything on the Internet or outside networks. Vandalism includes but is not limited to the intentional uploading, downloading, creating or transmitting of computer viruses, worms, Trojan horses, or other destructive program or applications.
7. **Security:** If users identify a security problem on the Network, such as evidence of hacking, users must notify a system administrator immediately. All users agree to cooperate with the District in the event of an investigation into any allegations of abuse or security breaches on the Network.
8. **Service Disclaimer:** The District makes no warranties of any kind, whether expressed or implied, for the Network services it provides. The District will not be responsible for any damages a user may suffer arising out of the user's use of, or inability to use, the Network, including but not limited to the loss of data resulting from delays, non-deliveries, mis-deliveries, service interruptions, or user error or omissions. The District is not responsible for the accuracy of information obtained through electronic information resources; hence, this information should be used at the user's own risk.
9. **Violations of This Policy:** Violations of this Policy may result in disciplinary action, including but not limited to restriction or termination of access to the Network, and/or other discipline in accordance with the applicable Student Conduct Policy, collective bargaining agreement or other Board policies. Violations also may be referred to the appropriate legal authorities and/or other legal action may be pursued.
10. **Signed Authorization Form:** There must be a signed Parent/Guardian Permission Form or Staff/Volunteer Agreement Form on file before the user gains access to the Network.

Parents/Guardians will complete the Parent/Guardian Permission Form upon registration for new students annually. The signed form will be kept in the student's cumulative folder.

Employees will complete the Staff/Volunteer Agreement form upon employment. The signed form will be kept in the employee's personnel file.

Adoption date: July 12, 2005