4.04 Acceptable Use of Technology Policy for School Staff/Students

Acceptable Use of Technology Policy for School Staff

Access to technology is provided as a privilege and as an employment tool. In order to continue enjoying access each staff member must take responsibility for appropriate and lawful use of this privilege. Staff members are responsible for professional behavior while using technology regardless if it is district owned or personally owned just as they are in a classroom, school hallway, or other school setting. While the School District may make reasonable efforts to supervise staff member use of technology access, the ultimate responsibility for exercising and promoting responsible use of this access is that of the staff member. Access to technology includes all devices either owned by the school district or the staff member. Networks include those provided by the school district or those not owned by the district that could be accessed by any staff owned device.

District network systems are defined as: hardware, software and data located on servers and/or local hard drives, Internet access, electronic messaging systems, IP or Internet-based telephone systems, and computerized access to data (local and online) for the use of the Staff Member as an employee of the District. As such this access will (1) assist in the collaboration and exchange of information, (2) provide opportunities to utilize technology for the analysis of district data, (3) facilitate personal growth in the use of technology, (4) enhance information gathering and communication skills, and (5) provide opportunities to utilize technology as a tool to increase student achievement. Personal network systems are defined but not limited to hardware, software, Internet access, voice/data access, or other technologies owned by the staff member but being used on the school premises during working and non-working hours.

Staff Members acknowledge by signing this agreement that they have read, understood, and will comply with the security and legal issues involved concerning access to the district network systems including but not limited to: Progress Book, DASL, Value Added data, Email, and other networked services online or local. The policy applies to all employees who use or otherwise access the Network either on-site or remotely. A copy of this policy shall be provided to staff members and available online on the district website.

Each staff member is responsible for reading and abiding by this policy. If you have any questions about the provisions of this policy, you should contact the administrator in your school building or the Technology Director. Any use of your account that violates this policy may result in your access being withdrawn and/or additional disciplinary action in accordance with any applicable state law, collective bargaining agreement and Board Policy.

1. ***Term of the Permitted Use***
   Access to technology is a privilege, not a right, and as such it may be suspended or revoked by the School District at any time. The School District may also limit access depending on student and staff schedules, equipment availability, or other constraints.

2. ***Authorized Users***

Network resources are only for use by authorized users. Anonymous use is not permitted, and access may not be shared or transferred. Staff members shall not share their passwords or otherwise allow anyone to gain unauthorized access to the Network or the Internet. Staff members are expected to maintain the security of their passwords. Usernames and passwords must be stored in a secure location and changed immediately if the staff member suspects anyone else has had access to them. Staff members should also notify the Technology Director if they believe that an account has been accessed without authorization. Staff members are expected to log out of all network applications (Examples: Progress Book, DASL, Value-Added, Email) whenever leaving their computer.

3. ***Acceptable Uses- Regardless of ownership of device or network***

    a. Locating and accessing educational resources.
    b. Direct use in instruction.
    c. Research for instructional and/or school management purposes.
    d. Collaboration with colleagues and other school personnel on instructional or management issues.
    e. Administrative announcements.
    f. General work-related communications.
    g. Union announcements and communications, to the extent authorized by any applicable collective bargaining agreement.
    h. Incidental personal use of e-mail, texting, instant message, and access to social media during non-work time to communicate with family, friends, and colleagues, provided such usage is limited in scope and is otherwise in compliance with this policy. For purposes of this paragraph, "incidental" use shall be defined as no more than ten (10) incidents during anyone day. Staff members should not utilize any network for exceptionally large data transfers such as photos, videos, streaming radio, streaming video, etc. Exceptions to this limitation may be permitted for personal emergencies and other extenuating circumstances.

4. ***Unacceptable Uses- Regardless of ownership of device or network***

Among the uses and activities that are known to be unacceptable and constitute a violation of this policy are the following:

    a. Uses or activities that violate the law or District policy, or that encourage others to violate the law or District policy, such as:
        i. Offering for sale or use or soliciting the purchase or provision of any substance the possession or use of which is prohibited by law or District policy.
        ii. Creating, copying, viewing, transmitting, downloading, uploading or seeking sexually oriented, sexually explicit, obscene, or pornographic materials.
        iii. Creating, copying, viewing, transmitting, downloading, or uploading any materials that include the design or information for the purposes of creating an explosive device, materials in furtherance of criminal activities

or terrorist acts, threatening materials or any other materials that violate or encourage others to violate the law or District policy.

iv. 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.

v. Copying, downloading, uploading or transmitting confidential information or trade secrets.

vi. Engaging in harassment, stalking, or other repetitive unwelcome communications, or using the Internet in support of such activities.

vii. Use of any device or network (district owned or privately owned) during work hours for activities not directly related to the duties of the employee beyond those as defined as incidental in acceptable uses.

b. Uses or activities that cause damage to the Network or to property. Among such uses or activities are the following:

i. Uploading, downloading, creating or transmitting to a district owned devices a virus, worm, Trojan horse, or other harmful component or corrupted data, or vandalizing the property of another. Vandalism includes any malicious attempt to hack, alter, harm or destroy software, hardware, data of another user, other District Network resources, or the use of the District Network to do any of the same acts on the Internet or outside Networks.

ii. Uploading, downloading, copying, redistributing or republishing copyrighted materials without permission from the owner of the copyright. Even if materials on the Network are not marked with the copyright symbol, you should assume that they are protected under copyright laws unless there is explicit permission on the Network.

c. Commercial uses. At no time may the network or the Internet be accessed for purposes of engaging in any kind of business or profit-making activity.

d. Use of technology unrelated to legitimate District purposes. Users may not, during the work day, access dating services or gaming web sites. Accessing sexually-oriented, sexually explicit, or pornographic material is strictly prohibited at all times. Use of the Network or Internet for any illegal activity is strictly prohibited at all times.

e. Using non-district e-mail. All use of e-mail should be through the School District's e-mail service. Accessing Internet-based e-mail providers (such as Hotmail or Google Mail) through the Network is allowed, but only during non-work hours and as such should be extremely limited. The district may at any time prohibit the use of non-district email should this become a detriment to the integrity of the network system or if it is being disruptive to staff productivity.

f. Uses that degrade or disrupt the operation of the Network or that waste limited computer, paper, or telephone resources. Examples include the extended streaming of audio or video content and the sending of unnecessarily large e-mail attachments. Printing documents that are non-school related. Utilizing the telephone for non-school issues.

g. Sending of messages to more persons than is necessary for school business purposes. This is a misuse of system resources and staff time and is prohibited. Large group mailings, such as "all staff' or "all building" are reserved for administrative use, subject to any exceptions which may be developed by the

school administration or system administrator. Users may not send a single e-mail message to more than ten (10) recipients without prior authorization. This limitation is subject to exceptions as may be developed by the administration or system administrator, or required by any applicable collective bargaining agreement. The use of multiple messages, non-system addresses, or other techniques to circumvent these limitations is strictly prohibited. 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.

Users wishing to distribute announcements regarding community activities, charitable activities or events, or other messages of general interest to the staff should contact their building administrator for permission. Any communication intended for an entire building or the district must be approved by the building administrator. At no time or under any circumstances should communications be made directly available to non-school persons or organizations.

h. 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 that makes message recipients believe that someone other than you is communicating or otherwise using the other's access to the Network.
i. Political activities: Creating, transmitting or downloading any materials that support or oppose the nomination or election of a candidate for public office or the passage of any ballot issue. Additionally, users shall not solicit political contributions through the network from any person or entity.
j. Installing or downloading software or hardware without the prior consent of a School District administrator or the system administrator. Staff members may not move, repair, reconfigure, modify or attach any external devices to Network equipment, computers or systems. Staff members shall not remove, alter or copy District software for their own personal use or for the use of others.

5. ***Common Courtesy Rules for E-mail Communications***

All users must abide by rules of common courtesy for e-mail communications. Among the uses and activities that violate these rules are the following:

a. Using inappropriate language, including swearing, vulgarities or other language that is suggestive, obscene, profane, abusive, belligerent, harassing, defamatory or threatening.
b. Using the Network to make, distribute or redistribute 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.
c. Forwarding or redistributing the private message of an e-mail sender to third parties or giving the sender's e-mail address to third parties without the permission of the sender.
d. Sending e-mail attachments that are too large to be accommodated by the recipient's system.

e. Using the network in a manner inconsistent with the professional expectations of a District employee. When using the network, users should remember that they are representing the District each time the account is used. Communications on the network need not be formal.

6. ***Data Security/ Personally Identifiable Information***

Users shall not remove or copy personally identifiable information for transportation away from the school site unless absolutely necessary for school business purposes, as set forth in the Code of Federal Regulations, Title 45, Family Educational Rights and Privacy Act (FERP A) and/or Ohio Rev. Code 3319.321. When it is necessary to transport personally identifiable information away from the school site, all reasonable precautions should be taken to protect against the loss, damage, or theft of such information, which may include encryption, passwording, and appropriate measures to ensure physical security.

Except as expressly set forth in this policy, users may release/display a student's personally identifiable information only to the student to whom it belongs or to the custodial parent/legal guardian. This complies with Ohio Rev. Code 3319.321. If in doubt, let your building office make this determination. Avoid using/releasing information for any research project. This complies with Code of Federal Regulations, Title 45, 20 U.S.C. § 1232g and 34 CFR Part 99.

Users must display/print personally identifiable information in secure conditions where and when unauthorized people will not have visual, auditory, or physical access to it. This includes:

- completely logging out of network applications when not in use.
- sending material to a network printer or copier only when it can be sure that the printed documents remain secure. This might mean printing from a computer next to the printer or having another staff member assist you in immediately retrieving such documents.
- maintaining printed lists and reports which release personally identifiable information only in secure locations.

7. ***Privacy***

Network access is provided as a tool for District business. The School District reserves the right to 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, communications and other content transmitted, received or stored in connection with this usage. All such information, content and files shall be and remain the property of the School District and you should not have any expectation of privacy regarding those materials. Network administrators may review files and intercept communications for any reason, including but not limited to for purposes of maintaining system integrity and ensuring that users are using the system in a manner consistent with this policy.

8. ***Web Sites, Social Media***

Web sites and social media sites created on the district website or an external site for district purposes must relate specifically to district sanctioned instruction, activities, programs or events. 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. All external

web sites created for education or informational purposes shall include a link back to the main district website.

9. ***Failure to Follow Policy***

Your use of technology is a privilege, not a right. As in the case of any District policy, your violation of this policy may result in disciplinary action, subject to the provisions of any applicable law or collective bargaining agreement. Your access to technology may be terminated, which the School District may refuse to reinstate for the remainder of your employment by the School District. Note also that it is a violation of this policy to fail to report violations of other users that come to your attention. It is a violation of this policy to use any electronic technology, including but not limited to any software, hardware, or externally provided service in an effort to disguise a user's network or internet activities that would otherwise be a violation of this Policy. It is a violation of this policy to utilize any device, practice, technique, or technological application for the purpose of avoiding or circumventing the provisions of this policy.

10. ***Warranties***

The School District makes no warranties of any kind, either express or implied, in connection with its provision of access to or use of its Network. It shall not be responsible for any claims, losses, damages or costs (including attorneys' fees) of any kind suffered, directly or indirectly, by any staff member arising out of the staff member's use of, or inability to use, the Network. Each staff member is responsible for backing up his or her files. The School District is not responsible for the accuracy of information obtained through electronic information resources, and this information should be used at the staff member's own risk.

11. ***Updates***

You may be asked from time to time to provide new or additional registration and account information to reflect developments in the law or technology. You must provide this information 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 the Technology Director or other person designated by the School District to receive this information.

12. ***Use of Third-Party Vendor Applications***

A third-party vendor application is a non-District website, online software, online application, online storage space, online cloud, or any other electronic service that holds user information accessible to the non-District entity.

Before using a third-party vendor's application to store, maintain, or transfer student education records, staff members must obtain approval from the principal in accordance with Board Policy 6.20. The Technology Director shall maintain a list of approved third-party vendors to whom the District has outsourced services or functions. These approved third-party vendors may have access to student education records as needed to perform the specific services and functions that have been approved. All questions regarding approved third-party vendors or approved services and functions of a vendor should be directed to the building administrator or the Technology Director.

Staff members may not use unapproved third-party vendors to store, maintain, or transfer student education records. Accordingly, any student information stored, maintained, or transferred via an unapproved third-party vendor application must be made anonymous. Student information is considered anonymous when a reasonable person in the community could not connect the information to a particular student with reasonable certainty. If a staff member is ever in doubt as to whether information is anonymous, he or she should consult the building administrator or the Technology Director.

Legal Ref.: ORC 3313.20, 3313.47, 3319.321, Code of Federal Regulations, Title 45, 20 U.S.C. § 1232g; 34 CFR Part 99, *Children's internet Protection Act of 2000*, 47 USC § 254 (h), (l)

Board Approved July 17, 2014