Book	Policy Manual
Section	800 Operations
Title	Acceptable Use of Internet
Code	815
Status	Active
Legal	1. Pol. 814
Adopted	April 15, 2009
Last Revised	June 12, 2019

Purpose

The Claysburg-Kimmel school District provides its employees, students, and other authorized individuals access to technology resources including, but not limited to, electronic communications systems, computers, computer networks, networked devices, hardware, software, internet access, mobile devices, peripherals, copiers, cameras, and cloud or web-based technologies.

The Board supports use of the district's technology resources to facilitate teaching and learning, to provide access to information, to aid in research and collaboration, to foster the education mission of the district, and to carry out the legitimate business and operation of the district.

The use of the district's technology resources is for appropriate school-related educational and operational purposes and for the performance of job duties consistent with the educational mission of the district. Use for educational purposes is defined as use that is consistent with the curriculum adopted by the district as well as the varied instructional needs, learning styles, abilities and developmental levels of students. All use for any purpose must comply with this policy and all other applicable codes of conduct, policies, procedures, and rules and must not cause damage to the district's technology resources.

All employees and students are responsible fot eh appropriate and lawful use of the district's technology resources. This policy is intended to ensure that all users continue to enjoy access to the district's technology resources and that such resources are utilized in an appropriate manner and for legitimate purposes.

For instructional purposes, the use of network facilities shall be consistent with the curriculum adopted by the school district as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.

Authority

The availability of access to electronic information does not imply endorsement by the district of the content, nor does the district guarantee the accuracy of information received. The district shall not be responsible for any information that may be lost, damaged or unavailable when using district

technology resources or for any information that is retrieved via the Internet. The district makes no warranties of any kind, whether express or implied, for the service it is providing through its various technology resources.

The district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet or other district technology resources.

The Board declares that access to and use of district technology resources is a privilege, not a right. The district's computer and network resources are the property of the district. Users shall have no expectation of privacy in anything they create, store, send, receive, delete or display on or over the district's Internet, computers or network resources, including personal files or any use of the district's Internet, computers or technology resources. The district reserves the right monitor, track, and log network access and use; monitor file server space utilization by district users;or deny access to prevent unauthorized, inappropriate or illegal activity and may revoke access privileges and/or administer appropriate disciplinary action. The district shall cooperate to the extent legally required with the ISP, local, state and federal officials in any investigation concerning or related to the misuse of the district's Internet, computers and network resources.

The Board requires all users to fully comply with this policy and to immediately report any violations or suspicious activities to the Superintendent or designee.

The Board establishes the following materials, in addition to those stated in law and defined in this policy, that are inappropriate for access by minors:

1. Defamatory.
2. Lewd, vulgar, or profane.
3. Threatening
4. Harassing or discriminatory.
5. Bullying.
6. Terroristic.

The district reserves the right to restrict access to any Internet sites or functions it deems inappropriate through established Board policy, or the use of software and/or online server blocking. Specifically, the district operates and enforces a technology protection measure(s) that blocks or filters access to inappropriate matter by minors on its computers used and accessible to adults and students. The technology protection measure shall be enforced during use of computers with Internet access.

Upon request by students or staff, the Superintendent or designee shall expedite a review and may authorize the disabling of Internet blocking/filtering software to enable access to material that is blocked through technology protection measures but is not prohibited by this policy.

Upon request by students or staff, building administrators may authorize the temporary disabling of Internet blocking/filtering software to enable access for bona fide research or for other lawful purposes. Written permission from the parent/guardian is required prior to disabling Internet blocking/filtering software for a student's use. If a request for temporary disabling of Internet blocking/filtering software is denied, the requesting student or staff member may appeal the denial to the Superintendent or designee for expedited review.

Upon request by teachers to the IT Department for temporary or permanent unblocking of a site for class use or assignment, the site will be checked and unblocking verified with the principal if appropriate, unblocked for use until the project or assignment is completed.

Delegation of Responsibility

The district shall make every effort to ensure that this resource is used responsibly by students and staff.

The district shall inform staff, students, parents/guardians and other users about this policy through employee and student handbooks, posting on the district website, and by other appropriate methods. A copy of this policy shall be provided to parents/guardians, upon written request.

Prior to being given access to district technology resources, users must sign agreements acknowledging awareness of the provisions of this policy, and awareness that the district uses technologies to monitor and detect inappropriate use on and off school property.

Student user agreements shall also be signed by a parent/guardian.

Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discern among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals.

Students, staff and other authorized individuals have the responsibility to respect and protect the rights of every other user in the district and on the Internet.

Building administrators shall make initial determinations of whether inappropriate use has occurred.

The Superintendent or designee shall be responsible for recommending technology and developing procedures used to determine whether the district's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedures shall include but not be limited to:

1. Utilizing a technology protection measure tht blocks or filters Internet access for minors and adults to certain visual depictions that are obscene, child pornography, harmful to minors with respect to use by minors, or determined inappropriate for use by minors by the Board.

2. Maintaining and securing a usage log.

3. Monitoring online activities of minors.

The Superintendent or designee shall develop and implement curriculum that ensures students are educated on network etiquette, digital citizenship and other appropriate online behavior, including:

1. Interaction with other individuals on social networking web sites and in chat rooms.

2. Cyberbullying awareness and response.

Guidelines

Un-Authorized Use Prohibited

Only users wh have agreed to abide by the terms of this policy may utilize the district's technology resources. Unauthorized use, utilizing another user's district account, or exceeding one's authorization to use district technology resources is prohibited.

Use of Personal Electronic Devices

The use of personal electronic devices on the district network is permitted only on designated networks. When a user connects a personal electronic device to a district network or district technology resource, this policy and its guidelines apply. Users are subject to the same levels of monitoring and access as if a district-owned device were being utilized. Users who connect a personal electronic device to a district network explicitly waive any expectation of privacy in the content exchanged over the district technology resources.

Privacy

The district reserves the right to monitor any user's utilization of district technology resources. Users have no expectation of privacy while using district technology resources whether on or off district property. The district may monitor, inspect, copy, and review any and all usage of district technology resources including information transmitted and received via the Internet to ensure compliance with this and other district policies, and state and federal law. All e-mails and messages, as well as any files stored on district technology resources, and other cloud or web-based applications, may be inspected at any time for any reason.

Internet Filtering and CIPA Compliance

The district utilizes content and message filters to prevent users from accessing material through district technology resources that has been determined to be obscene, offensive, pornographic, harmful to minors, or otherwise inconsistent with the district's educational mission. The Superintendent or his/her designee shall establish a procedure for users to request that a legitimate website or educational resource not be blocked by the district's filters for a bona fide educational purpose. Such requests must be either granted or rejected within three school days pursuant to the established procedure.

The Board directs that the Superintendent or his/her designee ensure that students at the elementary and secondary school levels are educated about appropriate online behavior including interacting via social networks and in chat rooms, cyber-bullying, and disclosure of personal information.

Monitoring

district technology resources shall be periodically monitored to ensure compliance with this and other district policies including monitoring of users' online activities. The network administrator designated by the Superintendent shall ensure that regular monitoring is completed pursuant to this section. However, the Superintendent, or his/her designee, shall also implement procedures to ensure that district technology resources are not utilized to track the whereabouts or movements of individuals, and that remotely activated location software and/or screen capturing is not utilized except where necessary to recover lost of stolen district technology.

District Provided Resources

District technology resources may be assigned or allocated to an individual user for his or her use (e.g., individual e-mail accounts, laptop computers, etc.). Despite being allocated to a particular user, the technology resources remain the property of the district and may be revoked, suspended, or inspected at any time to ensure compliance with this and other district policies. Users do not have an expectation of privacy in any district provided technology resource or any of its contents.

Safety

It is the district's goal to protect users from harassment and unwanted or unsolicited electronic communications. Any user who receives threatening or unwelcome electronic communications or inadvertently visits or accesses an inappropriate site shall report such immediately to a teacher or administrator. Users shall not reveal personal information to other uses on district technology resources, including chat rooms, e-mail, social networking web sties, ets...

Internet safety measures shall effectively address the following:

1. Control of access by minors to inappropriate matter on the Internet and World Wide Web.
2. Safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications.
3. Prevention of unauthorized online access by minors, including"hacking" and other unlawful activities.
4. Unauthorized disclosure, use, and dissemination of personal information regarding minors.
5. Restriction of minor's access to materials harmful to them.

Prohibitions

Users are expected to act in a responsible, ethical and legal manner in accordance with district policy, accepted rules of network etiquette, digital citizenship, and federal and state law. Specifically, the following uses of district technology resources are prohibited:

1. Use of technology resources to violate the law, facilitate illegal activity, or to encourage others to do so.
2. Use of technology resources for commercial or for-profit purposes.
3. Use of technology resources for non-school and non-business work.
4. Use of technology resources for political lobbying/campaigning or advertisement, not including student elections (e.g., student government, club officers, homecoming queen, etc...).
5. Use of technology resources to bully/cyberbully, or to communicate terroristic threats, discriminatory remarks,offensive or inflammatory communication, or hate.
6. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
7. Accessing, sending, receiving, transferring, viewing, sharing or downloading obscene, pornographic, lewd, or otherwise illegal materials, image or photographs.
8. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.
9. Use of technology resources to communicate words, photos, videos, or other depictions that are obscene, indecent, vulgar, rude, profane, or that advocate illegal drug use.
10. Use of technology resources to intentionally obtain or modify of files, passwords, and/or data belonging to other users or to the district.
11. Use that conceals or attempts to conceal a user's identity, including the use of anonymizers, pseudonyms, of the Impersonation of another user.
12. Fraudulent copying, communications, or modification of materials in violation of copyright laws.
13. Loading or usie of unauthorized games, programs, files, or other electronic media.
14. Use of technology resources to violate any other district policy.
15. Use of technology resources to engage in any intentional act which might threaten the health, safety, or welfare of any person or persons.D
16. Use of technology resources to cause, or threaten to cause harm to others or damage to their property.
17. Use of technology resources to attempt to interfere with or disrupt other users or district technology systems, networks, services, or equipment including, but not limited to, the

propagation of computer "viruses" and "worms", Trojan House and trapdoor program codes.
18. Destruction, modification, abuse or unauthorized access to district technology resources.
19. The use of proxies, VPNs, or other means to bypass internet content filters and monitoring.
20. Use of district technology resources to tether or otherwise connect to a non-district owned device to access and unfiltered and/or unmonitored internet connection.
21. Unauthorized access, interference, possession, or distribution of confidential or private information.
22. altering or attempting to alter other users' or system files, system security software, system or component settings, or the systems themselves, without authorization.
23. Use of technology resources in a manner tht jeopardizes the security of the district's technology resources, or in a manner that attempts to circumvent any system security measures.
24. Using technology resources to send any district information to another party, except in the ordinary course of business as necessary or appropriate for the advancement of the district's business or educational interests.
25. Use of technology resources to commit plagiarism.
26. Copying district software without express authorization from a member of the district's technology staff.
27. The use of technology resources to gamble.
28. Unauthorized access into a restricted system or changing settings or access rights to a restricted system or account.
29. The use of encryption software that has not been previously approved by the district.
30. Sending unsolicited mass-email messages, also known as spam.
31. Scanning the district's technology resources for security vulnerabilities.

Security

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or district files. To protect the integrity of the system, the following guidelines shall be followed:

1. Employees and students shall not reveal their passwords to another individual.

2. Users are not to use a computer that has been logged in under another student's or employee's name.

3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to district technology resources.

Copyright

The illegal use of copyright materials is prohibited. Any data uploaded to or downloaded from district technology resources shall be subject to fair use guidelines and applicable laws and regulations.[1]

Consequences for Inappropriate Use

Users shall be financially responsible for expenses related to repairs or replacements due to any damage, vandalism, loss or theft of equipment, systems, software, and all other district technology resources resulting from accidental, negligent, deliberate, or willful acts. The IT department will assess the damage and prepare costs needed to repair or replace. Parents/Guardian/Student will receive an invoice of cost and description of the repair or replacement, and record of the invoice sent and payments received will be kept at the school building in student records. All fees must be paid before participating in school-related events, attendance in school-related events including graduation, participation in extra-curricular activities, and issuing of diploma.

Illegal use of the district technology resources; intentional deletion or damage to files orf data belonging to others; copyright violations; and theft of services shall be reported to the appropriate legal authorities for possible prosecution.

General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy.

Vandalism will result in loss of access privileges, disciplinary action, and/or legal proceedings. **Vandalism** is defined as any malicious attempt to harm or destroy data of another user or district technology resources; this includes but is not limited to uploading or creating computer viruses.

Failure to comply with this policy or inappropriate use of district technology resources shall result in usage restrictions, loss of access privileges, disciplinary action, and/or legal proceedings.

Policy # 815 Attachment 2.doc (28 KB) 815-Attach 1.doc (22 KB)