CCHS Authorized Use Policy

Each student and his or her parent(s)/guardian(s) must sign the Authorization before being granted access. This Authorization need only be submitted once while enrolled at Carbondale Community High School District 165. Please read this document carefully before signing.

This Authorized Use Policy does not attempt to state all required or proscribed behavior by users. However, some specific examples are provided. The failure of any user to follow the terms of the Authorized Use Policy (AUP) will result in the loss of privileges, disciplinary action, and/or appropriate legal action. The signature(s) at the end of this document is legally binding and indicates the party who signed has read the terms and conditions carefully and understands their significance.

This Authorized Use Policy will apply to both school equipment and personal technology equipment used in the school building. This will include notebook computers, personal data assistants (PDA), USB devices such as flash drives or external hard drives, memory cards, digital cameras, cellular telephones, MP3 players, and any wireless access devices. Any new technologies will also be covered by this policy.

Purpose

The Board supports the use of the Internet and other computer networks in the district's instructional program in order to facilitate learning and teaching through interpersonal communications, access to information, research and collaboration.

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

Authority

The electronic information available to students and staff does not imply endorsement of the content by the school district, nor does the district guarantee the accuracy of information received on the Internet. The district shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet.

The school district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet, including telephone charges, and/or equipment or line costs.

The district reserves the right to log network use and to monitor fileserver space utilization by district users, while respecting the privacy rights of both district users and outside users.

The Board establishes that use of the Internet is a privilege, not a right; inappropriate, unauthorized and illegal use will result in the cancellation of those privileges and appropriate disciplinary action.

The Building Principal, and/or his designee will make all decisions regarding whether or not a user has violated the authorization and may deny, revoke, or suspend access at any time.

Guidelines

Network accounts will be used only by the authorized owner of the account for its authorized purpose. All communications and information accessible via the network should be assumed to be private property and shall not be disclosed. Network users shall respect the privacy of other users on the system.

Responsibility

The district shall make every effort to ensure that this educational resource is used responsibly by students and staff. Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discriminate 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 and staff have the responsibility to respect and protect the right of every other user in the district and on the Internet.

The building administrator shall have the authority to determine what is inappropriate use, and his/her decision is final.

Prohibitions

Students and staff are expected to act in a responsible, ethical and legal manner in accordance with district policy, accepted rules of network etiquette, and federal and State law. Specifically, the following uses are prohibited:

1. Use of the network to facilitate illegal activity.
2. Use of the network for commercial or for-profit purposes.
3. Use of the network for non-work or non-school related work.
4. Use of the network for product advertisement or political lobbying.
5. Use of the network for accessing, submitting, posting, publishing, or displaying inappropriate materials through e-mail, blogs, web pages and social sites. This would include discriminatory remarks, and offensive or inflammatory communication including inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material.
6. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
7. Use of the network to access obscene or pornographic material.
8. Use of inappropriate language or profanity on the network.
9. Use of the network to transmit material likely to be offensive or objectionable to recipients.
10. Use of the network to intentionally obtain or modify files, passwords, and data belonging to other users.
11. Impersonation of another user, anonymity, and pseudonyms.
12. Use of network facilities for fraudulent copying, communications, or modification of materials in violation of copyright laws.
13. Loading or use of unauthorized games, programs, files, or other electronic media.
14. Use of the network to disrupt the work of other users.
15. Destruction, modification, or abuse of network hardware and software.
16. Quoting personal communications in a public forum without the original author's prior consent.
17. Wasteful use of resources, such as disk space or printer supplies.
18. Gaining unauthorized access to resources or entities.
19. Using the network while access privileges are suspended or revoked.
20. Attempting to bypass network security, filters, and firewalls including the use of a proxy server.

Copyright

The illegal use of copyrighted software by students and staff is prohibited. Any uploaded to or downloaded from the network shall be subject to "fair use" guidelines.

Security

System security is protected through the use of passwords and monitoring software. 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 another student's or teacher'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 the network.
4. Recognize that electronic mail (E-mail) is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.
5. If you can identify a security problem on the Internet or Network, you must notify the Building Principal or System Administrator. Do not demonstrate the problem to other users.
6. Attempts to log on to the network as a system administrator will result in cancellation of user privileges.
7. Security and monitoring software is used to track network usage, troubleshoot problems, monitor appropriate use of technology, and restrict Internet access when needed.

Safety

To the greatest extent possible, users of the network will be protected from harassment or unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications shall immediately bring them to the attention of a teacher or administrator.

Network users shall not reveal personal addresses or telephone numbers to other users on the network.

Consequences For Inappropriate Use

The network user shall be responsible for damages to equipment, systems, and software resulting from deliberate or willful acts.

Illegal use of the network; intentional deletion or damage to files of data belonging to others; copyrighting violations or theft of services will 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. Loss of access and other disciplinary actions shall be consequences for inappropriate use.

Vandalism will result in cancellation of access privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks. This includes but is not limited to the uploading or creation of computer viruses.

Indemnification

The user agrees to indemnify the School District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any breach of this Authorized Use Policy.

Inspection

The equipment and access to the network and Internet remains the property and responsibility of the School District, which offers it to students and faculty for their convenience and educational use. The District reserves the right to limit use and to inspect the contents of files.