Title	Guest User Policy
Designation	KFD*

General Information

Internet connectivity has become a mandatory service in our schools. Like other school districts, we must provide safe, regulated access for all devices to make use of the expanding number of resources available to our students and staff. We are also willing to provide access to district guests who may access our network as a parent, community member or in some other capacity Providing guest internet (including wireless) access to our students, staff, and other visitors can help improve communication, collaboration, critical thinking and problem solving skills.

The district network is the property of the district and guest access is a privilege. The district assumes no liability for any damage or malfunction that may occur while or after using the guest network. In addition, the guest network is unsupported—meaning that we will not provide technical assistance to help users connect to or otherwise use our guest network. To keep our network safe we will regulate our guest access. Our desire to ensure smooth operation of our network relies upon users adhering to specific protocols and limitations. In order to be granted access to the district's network, a user must agree to the provisions of the district's policies and regulations governing network use—which are typically documented in a network user agreement (NUA). In general, the NUA require guests to agree to use our network in ways that are efficient, ethical, and legal. If a user violates the NUA, or other relevant regulations, procedures or guidelines, the district may revoke access to the network and may take other legal or disciplinary action. If necessary, the district will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the district network. Attempts to degrade or disrupt system performance will be viewed as violations of district policy and the NUA.

The guest network will be limited to bandwidth and connectivity resources that are not essential to district operations. Only Board members, staff members, and students enrolled in the district will be granted access to the district's primary, non-guest user network. District administrators may make occasional exceptions to include individuals in the employ of other agencies who are routinely on duty at a school site and who provide direct services to district students and/or teachers or guests who are involved in an educational activity at a district function. An appropriate zone leader or central office administrator must approve the exception prior to activation. In nearly all cases, procedures for access to the district network will be managed and maintained by district technology services.

Unless otherwise indicated by Human Resources, compliance with the NUA is a condition of employment Falcon School district 49.

Guests who accept the terms of the NUA will:

- Use the district network in support of educational and administrative objectives and in a way that is consistent with the mission and curriculum of Falcon School district 49.
- Abide by local, state, and federal laws such as, but not limited to, the Copyright Law, licensing laws, privacy laws, and district policies and regulations, as well as district and school-based guidelines.
- Abide by the acceptable use agreement referenced in BOE policy.
- Be responsible for maintaining confidentiality of passwords and protecting accounts from misuse.
- Ensure electronic communication sent from any non-district account will meet district requirements for acceptable use.
- Access network systems only when permitted by the owner of the account or with prior administrator authorization.
- Access the district network only through district-approved resources and/or services.
- Remain responsible for any physical or virtual damage done to the Falcon School district network, software, data, user accounts, hardware and for any unauthorized costs.

Users will not:

- Use the wireless guest network to create or expand the network—granting access to other users.
- Use the district wireless guest network to harass any person on the basis of race, color, sex, religion, national origin, age, disability, or any other basis. (district policies and regulations prohibiting harassment apply to the use of the district wireless guest network.)
- Use the district wireless guest network to access, process, generate, or distribute pornographic or obscene material, inappropriate text or graphic files, files which may be harmful to themselves and others, or files dangerous to the integrity of the Falcon School district network.
- Attempt to circumvent security measures or filters.
- Load, install, redistribute or access software on district assets without permission from district Technology Services (i.e., open source, unlicensed, or illegal).
- Install hardware into the network that is not owned and licensed by the district.
- Use the district network for private financial gain, commercial advertising, or solicitation purposes.
- Use the district network to solicit, proselytize, advocate or communicate the views of any non-school sponsored organization, or to raise or solicit funds for any non-school related or non-school sponsored entity or organization, whether for profit or non-profit.
- Use the district network to establish any non-approved website.
- Perform an act that plagiarizes the work of another without express consent.
- Participate in any form of slander.
- Pretend to be someone else when sending/receiving electronic communications.
- Reveal personal information such as addresses or phone numbers of the user or others.
- Use the district network in such a way that would disrupt the use of the district network by other users.
- Send frivolous or excessive messages and images.
- Create, send, or forward chain letters or any other message type that causes district network congestion or interferes with the delivery of electronic communication to others.
- Send electronic communication to anyone who asks you not to.
- Forge or attempt to forge electronic messages.
- Attempt to read, delete, copy, or modify the electronic communication of other system users or interfere with the ability of other system users to send/receive electronic communication.
- Download attachments into the district system that do not meet these responsible use guidelines.
- Host unofficial and unauthorized resources represented as district websites.

Additional Conditions

- The district reserves the right to access, retrieve, print, read, disclose to third parties or otherwise monitor (i) all messages (including personal messages) sent or received through its electronic communications system; (ii) all sites visited and files downloaded on the Internet; and (iii) all other uses of the district network.
- Reasons for which the district or others authorized by it may access such information include, but are not limited to: (i) to provide for the safety and security of minors; (ii) to determine whether a violation of this policy or other district policies has occurred; (iii) to investigate and repair a failure or error in the network system; or (iv) to obtain information requested by a third party in litigation or in response to a government investigation.
- Messages sent over the district network (including personal messages) and other uses of the district network should not be considered private or confidential.
- Use of the district network constitutes consent to access by the district or others authorized by it to electronic messages sent and received, to sites visited on and files downloaded from the Internet and to all other uses of the district network.
- Electronic communication sent or received by the Board, district employees or students, including electronic communications on district- owned equipment, as well as other documents generated through use of the district network, may be considered a public record subject to disclosure or inspection under the Colorado Open Records Act.

Teachers monitoring student use of network shall:

- Review with students the district network policies, regulations, and responsible use guidelines, to include Internet safety information, guidelines for appropriate online behavior including use of social networks, and cyberbullying awareness and response, as well as applicable acceptable use agreements.
- Report to appropriate district personnel any inappropriate materials that are found to be accessible.
- Report to appropriate district personnel inappropriate behavior. Report any attempt to harm or destroy any district equipment or materials, data of another user of the district system, or any other networks.
- Prohibit and report any harm or destruction that is the result of negligence to any district equipment or materials, the data of another user of the district system, or any other networks.

- Adopted: October 10, 2013

LEGAL REFS:

- C.R.S. 16-22-102(9) *(unlawful sexual behavior)*
- C.R.S. 22-32-109.1 (2)(a) *(adoption and enforcement* of *discipline code)*
- C.R.S. 22-32-109.1 (2)(a)(I)(E) *(policy required as part* of conduct and discipline code*)*
- C.R.S. 22-33-1 05 *(suspension, expulsion, and denial* of *admission)*
- C.R.S. 22-33-106 *(grounds for suspension, expulsion, and denial* of *admission)*

CROSS REFS:

- JIC and subcodes, Student Conduct
- JIH, Student Interviews, Interrogations and Searches
- JK and subcodes, Student Discipline