Jeffco Public Schools Acceptable Use Policy

Student Use of District Computing Resources and the Internet

The district believes the all district computing resources, applications and the Internet should be used in schools as learning resources to educate and to inform students. Accordingly, the district provides access to the Internet for its students as a means to offer a wide variety of educational resources. While many opportunities offered by the Internet are exciting and appropriate, others are unsuitable for school use. Consequently, use of all district provided computing resources and the Internet is for educational purposes only while attending school.

The Internet is a fluid environment in which information available to students is constantly changing. The district acknowledges that it is impossible to predict with certainty what information students might locate. The electronic information available to students does not imply endorsement by the district of the content, nor does the district make any guarantee as to the accuracy of information received on the Internet.

The district will make every reasonable effort to ensure that district and non-district provided educational resources are used appropriately and responsibly by students. To this end the district will provide content filtering devices and applications that control student access to inappropriate material on the Internet. Administrators, teachers, and staff have a professional responsibility to work together to help students develop the intellectual skills needed to evaluate and choose information sources, to identify information appropriate to their age and developmental levels, create effective and appropriate information, and to evaluate and use information to meet their educational goals.

Use of all educational resources demands personal responsibility and an understanding of the district's acceptable use procedures for the Internet. Student use of the Internet is a privilege, not a right, and therefore entails responsibility. General rules for behavior and communications apply when using all district provided computing resources, including the Internet. Failure to follow the district's acceptable use procedures and/or this policy will result in the loss of the privilege to use this educational tool and restitution for costs associated with damages, and may result in school disciplinary action (including suspension or expulsion) and/or legal action.

The district's Information Technology group may review student files and communications to maintain system integrity and to ensure that users are using the system appropriately and responsibly. Students shall have no expectation of privacy in any information stored on the district's servers, or in their use of school computers. The district reserves the right to monitor, inspect, copy, review and store (at any time and without prior notice) all usage of district computers and computer systems, including all internet and electronic communications access and transmission/receipt or materials and information.

Students and their parents/legal guardians shall be required to complete and sign the district's "Acceptable Use Agreement" prior to students being permitted to access the Internet at school. The completed and signed Agreements shall be kept on file with the school.

Prohibited Uses

No student shall access, create, transmit, retransmit or forward material or information that:

- promotes violence or advocates destruction of property including, but not limited to, access to information concerning the manufacturing or purchasing of destructive devices or weapons.
- is not related to district educational objectives except as provided in other district policies.
- contains pornographic, obscene or other sexually oriented materials, either as pictures or writings, which are intended to stimulate erotic feelings or appeal to prurient interests in nudity, sex or excretion.
- depicts, describes or represents in a potentially offensive way simulated sexual act or sexual content or a lewd exhibit of the genitals that, taken as a whole, lacks serious literary, artistic, political or scientific values.
- harasses, threatens, demeans, or promotes violence or hatred against another person or group of persons with regard to race, color, gender, sexual orientation, religion, national origin, age, marital status, disability or handicap. Sexual orientation is a person's orientation toward heterosexuality, homosexuality, bisexuality, or transgender status or perception of the individual's sexual orientation.

- plagiarizes the work of another.
- uses inappropriate or profane language or depictions likely to offend or intimidate others in the school community.
- is knowingly false or could be construed as intending to purposely damage another person's reputation.
- violates any federal or state law, including but not limited to copyrighted material and material protected by trade secret that contains personal information about themselves or others, including information protected by confidentiality laws.
- impersonates another or transmits through an anonymous remailer.
- shares student or district staff home addresses, phone numbers, or other private information except as allowed in district policy JRA/JRC.

The following activities are also prohibited:

- Using another individual's internet, electronic communications, or other district specific assigned account.
- Unauthorized attempts to log in to any network as a system administrator.
- Any malicious attempt to harm or destroy Jefferson County Public School (JCPS) data, data of another user, or other JCPS computing facility.
- Downloading, installing, storing or using malicious software, viruses, 'cracking,' and keystroke monitoring software and/or hardware.
- Attempting to evade, disable, or 'crack' password or other security provisions of the systems on the network.
- Interfering with or disrupting another information technology user's work as well as the proper function of information processing and network services or equipment.
- Intercepting or altering network packets.
- Setting up any type of proxy server and connecting it to the district's network in an attempt to bypass web filtering and/or firewall rules.
- Using information systems or resources for personal use or gain.
- Sharing or loaning accounts: all computer/security accounts are for the use of the single individual, the person for whom the account was approved. Sharing or loaning accounts is prohibited.
- The individual assigned a computer/security account is accountable for any and all transactions entered under that computer/security account login.
- Leaving an active system unattended, thereby allowing an unauthorized person to gain access to district resources through the user's login session.
- Attempting to gain unauthorized access to any other computer/security accounts.
- Using a computer for unlawful purposes, such as the illegal copying or installation of software, or violation of copyright laws.
- Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws.
- Altering technology equipment (hardware or software).
- Accessing, viewing, or altering any official record or file of the school or district.

Sanctions

Sanctions for violations of any of the above prohibitions may include loss of access to district computing resources and/or Internet access, restitution for costs associated with damages, school disciplinary action (including suspension or expulsion), and legal action.