Fountain-Fort Carson School District 8
Acceptable Use Policy (AUP)

Introduction

The District's Acceptable Use Policy (AUP) is to prevent unauthorized access and other unlawful activities by users online, prevent unauthorized disclosure of or access to sensitive information, and to comply with the Children's Internet Protection Act ("CIPA"). In the interest of safety, the District shall educate students and/or parents about appropriate online behavior, including cyberbullying awareness and response, and interfacing on school networking sites and in chat rooms. As used in this policy, "user" includes anyone using computers, laptops, cell phones, Internet, email, chat rooms, instant messaging (IM), peer-2-peer (P2P), and other forms of direct electronic communications or equipment provided by the District referred to as the network or technology resources. This policy also covers any outside equipment that may use the District's network to access the Internet.

The District shall maintain official profiles on social networking sites of its choosing, which will be monitored and managed by District Communications staff, in collaboration with school and department designees. These accounts shall be maintained for the purpose of communicating about District and school news, issues and parent/public engagement.

Staff members should not communicate with students through personal platforms/applications (including social media). Staff who need to communicate with students regarding classwork or extracurricular information (including athletics) should do so only using pre-approved, authorized District communications/notifications tools where the principal and District staff have oversight and record of such communications. Staff members are expected to protect the health, safety and emotional well-being of students and to preserve the integrity of the learning environment.

Staff members are expected to serve as positive role models and must represent the school and District professionally at all times when engaging in online activity or conversations.

The District will use technological protection measures to block or filter, to the extent possible, access to materials that are obscene, pornographic, and harmful to minors over the network. The District reserves the right to monitor users' online activities and email communications, and to access, review, copy, and store or delete any electronic communication or files and disclose them to others as it deems necessary without the consent of the user. Users should have no expectation of privacy regarding their use of District technology resources including cell phones, computers and laptops, email communication, network and/or Internet access. Email messages created and transmitted via the District email system and/or network remain the property of the District.

Students

Schools must qualify students to use the District's technology resources at the beginning of each school year with a signed AUP. Students who are under 18 must have their parents or guardians sign the AUP and schools must keep the signature page on file. Once signed, the permission/acknowledgement page remains in effect until revoked by the parent, or the student loses the privilege of using the District's technology resources due to violation of the policy or is no longer a student of the District.

The District provides email, Internet access, and accounts for online services for the purpose of advancing the educational mission of the District. Email accounts will be provided to 4th-12th grade students; various online accounts will be provided to all students as needed, unless the student's parent/guardian has indicated in writing to the school that they prefer their child not have email. Use of educational resources, including email accounts, demands personal responsibility and an understanding of the acceptable use procedures for computers, networks, and Internet access. The District does not support student use of personal devices on the District network.

School/District officials will provide access to online services with educational partners/companies for the purpose of advancing the educational mission of the District. An approved list of educational partners who

possess safe student data privacy policies in compliance with the Colorado "Student Data Transparency and Security Act HB 16-1423" can be found on the District website. Providing access to online services may require the creation of student accounts in order for the student to access the educational content, resources, interactive features, authoring and or publishing capabilities provided by the online service.

The District will provide each student with appropriate access to such District approved online services listed on the District website, unless the student's parent/guardian has indicated in writing, by submitting a formal letter to the school's principal, that they prefer their child not have this access. If your student enrolls in college courses through Concurrent Enrollment, you hereby grant permission for your student to use any application or website that is used as part of the college course(s), some of which is only intended to be used by individuals 18 years of age or older.

Staff

Employees and other users are required to follow this policy. Even without a signature, all users must follow this policy and report any misuse of email, the network or Internet to a District Administrator. Access is provided primarily for education and District business. By using the District technology resources, users have agreed to this policy. If a user is uncertain about whether a particular use is acceptable or appropriate, he or she should consult a District Administrator.

District Issued Laptops

High school and middle school students and their parents/legal guardians should refer to the Laptop Contract provided by their school for specifications regarding proper use, repair and responsibilities. Laptop use must be in compliance with the District's Acceptable Use Policy. Staff members with District-issued laptops are required to follow listed guidelines regarding proper use, repair and responsibilities:

Maintenance and Repair

1. Any damage must be promptly reported and scheduled for repair.
2. All repairs are to be done only by the District's technical services department.
3. If damage occurs due to carelessness, user will be billed for the cost of the parts and/or laptop.
4. General cleaning and care of the laptop is the responsibility of the user.
5. Laptop must be transported in a suitable carrying case.
6. The laptop must not be left unsecured or unattended.

Storage of Files and Software

1. The District is not responsible for lost files and/or data. Users are encouraged to maintain separate backups of important data.
2. Personal software is not to be loaded onto the laptop at any time.

Lost or Stolen Equipment

1. Users are financially responsible if the laptop is lost or stolen.
2. A police report must be filed within 24 hours of incident.

Unacceptable Uses of the District's Network, Resources, or Online Services.

The following are examples of inappropriate activity on the District network, technology resources, Internet, email or Online Services.

- Violation of any state or federal law or municipal ordinance, such as: accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials.
- Criminal activities that can be punished under law.
- Selling or purchasing illegal items or substances.

- Obtaining and/or using anonymous email sites; spamming; spreading viruses.
- Causing harm to others or damage to their property, such as:
    1. Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials;
    2. Deleting, copying, modifying, or forging other users' names, emails, files, or data; disguising one's identity, impersonating other users, or sending anonymous email;
    3. Damaging computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance;
    4. Using any device to pursue "hacking," internal or external to the District, or attempting to access information protected by privacy laws; or
    5. Accessing, transmitting or downloading large files, including "chain letters" or any type of "pyramid schemes."
- Engaging in uses that jeopardize access or lead to unauthorized access into others' accounts or other computer networks, such as:
    1. Using another's account password(s) or identifier(s);
    2. Interfering with other users' ability to access their account(s); or
    3. Disclosing anyone's password to others or allowing them to use another's account(s).
- Using the network or Internet for commercial purposes such as:
    1. Personal financial gain;
    2. Personal advertising, promotion, or financial gain; or
    3. Conducting for-profit business activities and/or engaging in non-government related fundraising or public relations activities such as solicitation for religious purposes, lobbying for personal political purposes.

Penalties for Improper Use

The use of a District account is a privilege, not a right, and misuse will result in restriction or cancellation of the account. Misuse may also lead to disciplinary and/or legal action for both students and employees, including suspension, expulsion, dismissal from District employment, and/or criminal prosecution by government authorities. The District will attempt to tailor any disciplinary action to specific issues related to each violation.

The District reserves the right to take immediate action regarding unacceptable activities such as:

1. Those that create security and/or safety issues for the District, students, employees, schools, network or computer resources;
2. Those that expend District resources on content the District in its sole discretion determines lacks legitimate educational content/purpose; and
3. Other activities as determined by the District as inappropriate.

Disclaimer

The District makes no guarantees about the quality of services provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from use of the network or accounts. Any additional charges a user accrues due to the use of the District's network are to be borne by the user. The District also denies any responsibility for the accuracy or quality of the information obtained through user access. Any statement accessible on the computer network or Internet is understood to be the author's individual point of view and not that of the District, its affiliates, or employees.

Signature Page for Acceptable Use Policy

By signing below, I acknowledge to having read, understand, and agree to abide by, the provisions of the Acceptable Use Policy of Fountain-Fort Carson School District 8.

STAFF MEMBERS

School_____ Date_____

Staff Signature_____

Staff Name (please print)_____

STUDENTS AND PARENTS

Student Signature_____

Student Name (please print)_____

Parent/Guardian Signature_____

Parent/Guardian Name (please print)_____

Students/Parents – Please return this form to your school where it will be kept on file.

Staff – Please return this form to the Central Administration Office where it will be kept on file.

Agreement to the provisions of the AUP is required for all students and staff using the District Network, internet access and/or computers.