Edwards County Community Unit School District #1

Student Technology Acceptable Use Policy

**Please Read**

Please read this document carefully before signing. The signatures at the end of this document are legally binding and indicate that you have read this Technology Acceptable Use Policy (TAUP) and understand its significance. The failure of any user to follow the terms of the TAUP may result in the loss of privileges, disciplinary action, and/or appropriate legal action. Each student and his or her parent(s) / guardians must sign the TAUP before being allowed to utilize the school's technology resources. The TAUP need only be submitted annually while enrolled at Edwards County Community Unit School District #1.

It's a Guide to Acceptable Technology Usage

The TAUP is intended to be a usable guide to the proper use of technology in the District. It is not intended, nor can it be a comprehensive guide. However, some specific examples are provided to illustrate acceptable use. In summary, faculty 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.

All District, Personal, Current and Future Technology Services and Equipment in the School

The TAUP will apply to both school equipment and personal technology equipment used in or on school property. This will include computers, notebook computers, personal data assistants (PDA), USB devices such as flash drives, external hard drives, memory cards, digital cameras, cellular telephones, cell cameras, MP3 players and any wireless access devices. Any new technologies not mentioned by name in this document will also be covered by these policies.

Purpose

Edwards County Community Unit School District #1 supports the acceptable and beneficial use of technology, the Internet and other computer networks in the District's instructional program in order to facilitate teaching and learning consistent with the curriculum adopted by the Board. In these contexts, the Board recognizes the pedagogical benefits associated with technology applications related to interpersonal communications, access to information, research, collaboration, and the need to address varied instructional methods, learning styles, abilities and developmental levels of students.

General Concepts

1. Students are to treat all equipment with care and are to report instances of abuse or misuse as soon as the user becomes aware of the issue
2. The school's equipment, computer network and access to the Internet are the property of the School District and utilization of these resources is a privilege, not a right
3. In furtherance of the purposes outlined, the District reserves the right to implement appropriate action that includes, but is not limited to, the following:
    a) Limitation or cancellation of these privileges
    b) Disciplinary action and/or legal action
    c) Routine inspection of the contents of any transmissions that utilize these resources within current legal parameters
    d) Log network use and to monitor file server space utilization of District users

    e) Other restrictions or sanctions as necessary
4. The Building Principal and/or his/her designee will make all decisions regarding whether or not a student user has violated the TAUP and may deny, revoke or suspend access at any time.
5. The District shall not be responsible for any information that may be lost, damaged or unavailable when using technology resources or for any information that is retrieved via the Internet
6. The School District shall not be responsible for any unauthorized charges or fees resulting from access to the Internet

Privacy and Access Guidelines

1. Network accounts will be used only by the authorized owner of the account for its authorized purpose
2. Unless otherwise noted, all communications and information that are accessible via technology resources should be assumed to be private property of the District and shall not be disclosed to anyone without the written permission of the District or in accordance with current state and federal law
3. Network users shall respect the privacy of other users on the system

No Expectation of Privacy with Respect to School Email or Technology Resource Usage

1. Electronic mail (email) that is processed via the school's technology resources is not private. The District technology staff has access to all email, and they are authorized to periodically monitor Internet and school email usage
2. Students possess no expectation of privacy with respect to their email or internet usage processed through the school network
3. In addition to previously mentioned access, the District reserves the right to search otherwise private electronic records in those instances when they have reasonable suspicion that a violation of the law or school rules has occurred or where the safety of the school community is in question consistent with current legal precedents

Expected Behaviors – Responsible Technology Use

1. Students are expected to act in a responsible, ethical and legal manner in accordance with District policy, accepted rules of technology etiquette and federal and state law
2. The school community will help students 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
3. Any person who has knowledge of technology abuse or misuse has a responsibility to report it to the appropriate school personnel
4. Any technology user who receives threatening or unwelcome communication should immediately bring them to the attention of an administrator
5. Technology users should never reveal personal addresses, telephone numbers or other identifying information to people they do not know

Examples of Prohibited Behaviors

This TAUP prohibits the use of technology resources:

1. To facilitate activities that are illegal or contrary to school rules or policies
2. For commercial or for-profit purposes
3. For non-work or non-school related work

4. For product advertisement or political lobbying
5. For searching for, accessing, submitting, posting, publishing, downloading or displaying inappropriate materials by means of the Internet and/or email, 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 materials. In addition, users may not search for, access, submit, post, publish, download or display information by means of the Internet and/or email containing any of the following topics:

| | |
|---|---|
| Alcohol Bomb Making | Libelous or Slanderous Material |
| Deviant Social Behavior | Militants and/or Extremist Students or Groups |
| Gambling | Pornography and/or Sexually Oriented Material Profanity |
| Gangs | Racism |
| Human or Animal Mutilation | Satanic Themes and/or Cults Violence |
| Illegal Activity | Weapons |
| Illegal Drugs | |

6. To transmit material likely to be offensive or objectionable to recipients
7. For unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials
8. To intentionally obtain or modify files, passwords and data belonging to other users
9. To impersonate or represent another user. This includes the use of pseudonyms
10. To load or use unauthorized games, programs, files or other media
11. To disrupt the work of other users
12. To destroy, modify or abuse hardware and software
13. To quote personal communications in a public forum without the original author's prior consent
14. To waste resources, such as disk space or printer supplies
15. To gain unauthorized access to resources or entities
16. To use technology resources while access privileges are suspended or revokes
17. To attempt to bypass technology resource security, filters and firewalls including the use of a proxy server
18. Failing to exit the Internet, shut down or log off a computer after being instructed to do so by school personnel
19. To harass or stalk another person by means of the Internet or email
20. Transmitting personal information to an Internet or email
21. Posting or transmitting anonymous messages
22. To post or transmit material created by another person without authorization

This is not all-inclusive. Any other misuse of the Internet or the District's electronic network system or other electronic mediums, deemed inappropriate by school personnel, may result in disciplinary action and/or appropriate legal action.

<u>Password Security</u>

The system's security is protected through the use of passwords and monitoring software. Failure to adequately protect of update passwords could result in authorized access to personal or District files. In addition, the District employs security and monitoring software to track network usage, troubleshoot problems, monitor appropriate use of technology and restrict Internet access when needed. In addition to these efforts, the following guideline shall be followed:

1. 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 technology resources
4. Any user who identifies a security issue on the Internet or Network must notify the Building Principal or System Administrator immediately. Users may not demonstrate the problem to other users
5. Attempts to log on to technology resources as a system administrator will result in cancellation of user privileges

Possible Consequences for Inappropriate Use

1. The network user shall be responsible for damages to equipment, systems and software resulting from deliberate or willful acts
2. Illegal use of technology resources; 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
3. General rules and policies 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
4. 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
5. In the vent that any user vandalizes any District computer hardware or software, he/she or the legal parent/guardian, if the user is a minor, will be responsible to pay all repair and/or replacement costs. By signing this agreement, the user and/or parent/guardian expressly agrees to be responsible for payment of costs incurred
6. Any user, who damages, destroys or copies another person's data will be referred for appropriate discipline and may be suspended from or denied access to all computers
7. Any user who tampers with or attempts to gain access to computer data to which he/she has no security authorization is in violation of District policy. It will be considered equivalent to tampering with a teacher's written records or attempted to gain access to confidential student information
8. The user expressly 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 the TAUP

Student Email/Google Apps Policy

ECCUSD #1 has partnered with Google Apps for Education to provide email and learning tools to students. Google Apps account is subject to be reviewed by District Technology staff at any times. At the time of the student's graduation, the account and all data will be deleted. District staff and the School Board have carefully considered students' online safety in setting up the procedures and rules for student accounts.

Students should consider their school email as an extension of the classroom, subject to the same rules of respect and courtesy that we expect in school. All guidelines that are listed in the TAUP also apply to student email. Student email accounts should only be used for school related activities.

Filtering of Emails

School email accounts must comply with the Federal Children's Internet Protection Act (CIPA). Student emails will be filtered, just as Internet access at school is filtered, to ensure student safety online. Every email sent and received from

a school email account goes through filtering software that scans for language and images. Student email addresses will have restrictions on what can be received. Students may only send/receive messages from addresses inside the eccusd.org domain. ECCUSD and Google makes every effort to block inappropriate content; however; technology is every evolving. If a student receives any inappropriate emails, they should be reported to an administrator or teacher and forwarded to the Building Principal.