CYPRESS FAIRBANKS
INDEPENDENT SCHOOL DISTRICT
LEARN • EMPOWER • ACHIEVE • DREAM

Technology Services Acceptable Use Policy

All communications on the district's network are property of the Cypress-Fairbanks Independent School District. Users have no privacy expectations in the contents of their personal files or any of their use of the district's network. The district reserves the right to monitor, track and/or log user access, monitor and allocate fileserver space, and access and archive all user files.

The level of access that employees have to school computers, network, and Internet services shall be based upon specific employee job requirements and needs. For Users, the district's network must be used for education-related purposes and performance of district job duties. The policy does recognize that employees may use district technologies for "incidental" personal use, but there should be no expectation of privacy.

The policy defines incidental use as casual, insignificant, or occasional "that does not impact an employee's duties or impede educational operations."

The Cypress Fairbanks Independent School District establishes that network use is a privilege, not a right. Inappropriate, unauthorized and illegal use will result in cancellation of those privileges and appropriate disciplinary action. Offenders can be written up or *the offense* could be grounds for termination depending on the severity of the infraction. The district will cooperate to the extent legally required with Internet Service Provider (ISP), local, state, and federal officials in any investigation concerning or related to the misuse of the district's network.

Computer - includes any district-owned, leased or licensed hardware, software, or other technology used on district premises or at district events, or connected to the district network. Computer includes, but is not limited to: desktop and laptop computers, mobile devices (cell phones, mp3 players, tablets, pagers, etc.), printers, cables, and other peripherals including thumb and flash drives, specialized electronic equipment used for students' special educational purposes, and any other such technology developed.

Network - a system that links two (2) or more computer systems, including all components necessary to effect the operation, including, but not limited to: computers, copper and fiber cabling, wireless communications and links, equipment closets and enclosures, network electronics, telephone lines, printers and other peripherals including thumb and flash drives, storage media, software, and other computers and/or networks to which the network may be connected, such as the Internet or those of other institutions.

CYPRESS FAIRBANKS
INDEPENDENT SCHOOL DISTRICT
LEARN • EMPOWER • ACHIEVE • DREAM

Guidelines

Network accounts shall be used only by the authorized owner of the account for its approved purpose. Network users shall respect the privacy of other users on the system.

Prohibitions

Students and employees 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, the Code of Professional Practice and Ethics, and the Public School Code. Additionally, this expectation applies to all users of district-owned technology. Specifically, the following uses are prohibited, but not limited to:

1. Illegal activity.
2. Communication focused on commercial or for-profit purposes.
3. Communication of private/personal information of others.
4. Participation in online gaming and/or gambling.
5. Product advertisement or political lobbying.
6. Hate mail, discriminatory remarks and offensive, inflammatory, or inappropriate communication.
7. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
8. Access (send, receive, view, download, or transmit) to sexually suggestive, sexually explicit, obscene or pornographic material or child pornography.
9. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.
10. Use of inappropriate language or profanity.
11. Transmission of material likely to be offensive or objectionable to recipients.

12. Intentional retrieval or modification of files, passwords, and data belonging to other users.

13. Impersonation of another user or communicating anonymously with the intent to harass, threaten, bully or be disrespectful to another individual.

14. Fraudulent copying/reproduction, communications, or modification of materials in violation of copyright laws.

15. Loading or use of, or the attempt to load or use, unauthorized games, programs, files, or other electronic media. Such authorization may only be granted by a teacher or district administrator. For the security of the district's network, users should download such files only from reputable sites and only for educational purposes.

16. Disruption of the work of other users.

17. Destruction, modification, abuse or unauthorized access to network hardware, software and files.

18. Quoting, summarization or other recounting of personal communications in a public forum without the original author's prior consent.

19. Cyberbullying or any other type of harassment prohibited by law, the Student Code of Conduct, or Board Policy.

20. Using district technology for social networking with students beyond the educational program.

21. Texting, messaging or chatting with students for any other reason than for school-related communication.

CYPRESS FAIRBANKS
INDEPENDENT SCHOOL DISTRICT
LEARN • EMPOWER • ACHIEVE • DREAM

Security

System security is protected through the use of passwords. 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:

22. Employees and students shall not reveal their passwords to another individual.

23. Users are not to use a computer that has been logged in under another user's name. If a previous user has not logged off, the current user must immediately log out and then log back in under his/her own name and password.

24. Unauthorized access, including hacking and logging into the network using another individual's username and password, is strictly prohibited and will result in discipline and denial of privileges. Such unauthorized access may also result in criminal charges.

25. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

26. Users must create passwords that follow the guidelines for required syntax: eight (8) character minimum using a combination of numbers, letters, and special characters.

27. Users must regularly change their password when directed by district administration or state mandates.

28. IT department support personnel will have administrative rights via their login ids. It is a violation of security rules outlined here to share password or logins with administrative rights with anyone.

29. The Administrator login to the computer will be limited to personnel of the DII team. All other support staff will have access to tools and their login IDs to ensure that the computer can be serviced. Trying to extract password falls under hacking rule listed above.

30. Attempting to gain unauthorized access to the District's network resources or local admin account go beyond authorized access and is prohibited.

31. User network passwords prevent unauthorized individuals from accessing the district's network without permission, however, such passwords are not required for authorized IT administrators and other district administrators to access an individual account.

Signature_____CFISD ID#_____DATE_____