

FORT BEND INDEPENDENT SCHOOL DISTRICT

DISTRICT ACCEPTABLE USE POLICY FOR ACCESSING COMPUTERS AND ELECTRONIC COMMUNICATIONS SYSTEMS

Internet access is a privilege available to employees and other designated individuals of Fort Bend Independent School District (FBISD). The goal in providing this service is to promote educational excellence at FBISD by facilitating communications for resource sharing, collaborative work and innovation. Access to Internet resources also brings the possibility of encountering material that may not be considered to be of educational value in the context of the school setting. The District has taken precautions to restrict access to controversial materials; however, on a global network it is impossible to control all materials. Although an industrious user may discover controversial information, the valuable information and interaction available on this worldwide network far outweighs the possibility that users may procure material that is not consistent with District educational goals.

The successful operation of the network relies upon the proper conduct of the users who must adhere to strict guidelines. The following rules of acceptable use are provided so that users are aware of the ethical and legal responsibilities associated with the use of network resources.

Rules of Acceptable Use:

A. General Use:

- Access to the District's electronic communications system is a privilege, not a right. Noncompliance with applicable regulations may result in suspension or termination of privileges and other disciplinary action consistent with District policies.
- System users shall keep their passwords confidential.
- System users may not use another person's system account or E-mail account.

- Attempts to log in to any computer network beyond the user's authorized level of access may result in immediate cancellation of user privileges or other disciplinary action.
- Teachers may not allow students to access the network through a teacher account.
- Any infraction of the Acceptable Use Policy, by a student or employee, shall be reported by the building principal to the Chief Information Officer, the Director of Information Technology Services, the Director of Digital Learning, and the FBISD Staff Attorney.
- The District, in its sole discretion, has the right to determine who is or is not given access to the FBISD electronic communications systems.

B. Internet/Electronic Communications Use:

- Access to the District's electronic communications system, including the Internet, shall be made available to employees exclusively for instructional and administrative purposes and in accordance with administrative regulations.
- Use of the FBISD electronic communications systems shall not be considered confidential and is monitored 24 hours a day. There is no expectation of privacy. All Internet activity is recorded.
- Use for commercial activities or political lobbying is prohibited.
- Users are expected to abide by the generally accepted rules of network etiquette (netiquette). These include (but are not limited to) the following:
 1. Be polite; messages typed in capital letters are the computer equivalent of shouting and are considered rude.
 2. Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language is prohibited.
 3. Revealing personal addresses or phone numbers of others is prohibited.
 4. Revealing and/or sharing personal identifiable information (PII) of employees and/or students to unauthorized person(s) is strictly prohibited.
 5. Revealing and/or sharing personal health information (PHI) of employees and/or students to unauthorized person(s) is strictly prohibited.
- Using the network in such a way that would disrupt the use of the network by other users (such as chain letters or accessing real audio for extended periods of time) is prohibited.

C. Computer Ethics:

- Access, copying, or transmission of any material in violation of any U.S. or state regulation is strictly prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, pornography, or material protected by trade secret.
- Vandalism - Any malicious attempt to harm, modify, or destroy District equipment or materials, data of another user of the District's system, or any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance may be viewed as violations of District Policy and administrative procedures and, possibly as criminal activity under applicable state and federal laws. This includes, but is not limited to, the uploading or creating of computer viruses. Vandalism as defined above will result in the cancellation of system use privileges and will require restitution for costs associated with system restoration, hardware, or software costs.

D. Restrictions:

- Campus faculty members may not move computer equipment or peripheral devices such as printers or make modifications to computer hardware or configurations. (The campus Information Technology (IT) support staff is responsible for such changes and for maintaining a current inventory of all equipment and its location.) Loss of network account or E-mail privileges may result from violation of this policy.
- Installation of software must be accomplished through proper channels and procedures. Software shall be selected from the list of approved software found on the Information Technology web pages on the FBISD web site.
- Non-standard software that is not provided by the District may be installed with permission and assistance from the campus IT support staff; however, the employee will be required to keep the original End User License Agreement (EULA) in his/her files as long as the software remains installed. The employee will be responsible for any upgrade and patching of the software.
- All Web pages created for the FBISD Web site must comply with the Fort Bend ISD Internet and Web Standards and must be approved and posted by the designated campus Web Master.

Consequences: Violation of any of the policies described above may result in employee disciplinary action which could include:

- loss of network privileges
- written reprimand
- dismissal

Disclaimer of Liability:

The District shall not be liable for users' inappropriate use of electronic communication resources or violations of copyright restrictions, users' mistakes or negligence, or costs incurred by the user. The District shall not be responsible for ensuring the accuracy or usability of any information found on the Internet. The District does not warrant that the functions or services performed by or that the information or software contained on, the system will meet the system users' requirements or that the system will be uninterrupted or error-free.

For additional information regarding the District's Electronic Communication and Data Management policy [CQ (local)] and procedures [CQ-R] refer to the Fort Bend ISD Board Policy Manual.

Agreements

I understand and will abide by the Fort Bend ISD Acceptable Use Policy for Internet and Computer Systems. I have also read and understand the Student Acceptable Use Policy. (Instructional staff only) I further understand noncompliance with applicable rules and regulations may result in suspension or termination of privileges and other disciplinary action consistent with District policies. Violations of law may result in criminal prosecution as well as disciplinary action by the District.

I understand and will abide by the Fort Bend ISD Acceptable Use Policy for Internet and Computer Systems. I have also read and understand the Student Acceptable Use Policy. (Instructional staff only) I further understand noncompliance with applicable rules and regulations may result in suspension or termination of privileges and other disciplinary action consistent with District policies. Violations of law may result in criminal prosecution as well as disciplinary action by the District.