

Spring Branch ISD Acceptable Use Guidelines

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT

CQ
(LOCAL)

The Superintendent or designee shall implement, monitor, and evaluate electronic media resources for instructional and administrative purposes.

AVAILABILITY OF ACCESS

Access to the District's electronic communications and data storage systems, including but not limited to the Internet, electronic mail, file servers, and applications servers shall be made available to students and employees primarily for instructional and administrative purposes and in accordance with administrative regulations.

LIMITED PERSONAL USE

Limited personal use of the system shall be permitted if the use:

1. Imposes no tangible cost on the District;
2. Does not unduly burden or cause harm to the District's computer or network resources;
3. Has no adverse effect on an employee's job performance or on a student's academic performance; and
4. Is not for personal gain.

USE BY MEMBERS OF THE PUBLIC

Access to the District's electronic communications and data storage systems, including but not limited to the Internet, electronic mail, file servers, and applications servers may be made available to members of the public in accordance with administrative regulations. Such use may be permitted if the use:

1. imposes no measurable cost on the District; and
2. Does not unduly burden or cause harm to the District's computer or network resources.

Members of the public who are granted access shall be required to comply with all District rules, regulations, and policies governing appropriate use of the system.

ACCEPTABLE USE

The Superintendent or designee shall develop and implement administrative regulations, guidelines,

1. Students in grades 5 and below will be granted access to the

- District's system under the direction and guidance of a teacher/staff member with a classroom account, as appropriate.
2. Students in grades 6 – 12 will be assigned individual network accounts.
 3. As appropriate and with the written approval of the immediate supervisor, District employees will be granted access to the District's system.
 4. The District will require that all student passwords be changed at least annually. Other users will change passwords as required by the Chief Technology Officer.
 5. Student email accounts must be requested by the teacher and approved by the Principal of their designee.
 6. Any system user identified as a security risk or as having violated District and/or campus computer use guidelines may be denied access to the District's system.
 7. All users will be required to sign a user agreement annually for issuance or renewal of an individual account.

Internet Safety

The Chief Technology Officer for the District's electronic communications system (or designee) will:

1. Be responsible for disseminating and enforcing applicable District policies and acceptable use guidelines for the District's system.
2. Ensure that all users of the District's system complete and sign annually an agreement to abide by District policies and administrative regulations regarding such use. All such agreements will be maintained on file in the principal's or supervisor's office.
3. Ensure that employees supervising students who use the District's system provide training emphasizing the appropriate use of this resource.
4. Ensure that all software loaded on computers in the District is consistent with District standards and is properly licensed.
5. Be authorized to monitor or examine all system activities, including electronic mail transmissions, as deemed appropriate to ensure student safety on-line and proper use of the system.
6. Be authorized to disable a filtering device on the system for bona fide research or another lawful purpose, with approval from the Superintendent.
7. Be authorized to establish a retention schedule for electronic media and to remove media that are deemed to be inappropriate.
8. Set limits for data storage within the District's system, as needed.

Filtering

The following standards will apply to all users of the District's electronic information/communications systems:

Monitored Use

1. The individual in whose name a system account is issued will be responsible at all times for its proper use.
2. The system may not be used for illegal or commercial purposes or for any other activity prohibited by District policy or guidelines.
3. System users may not disable, or attempt to disable, a filtering device on the District's electronic communications system.
4. Communications may not be encrypted so as to avoid security review by system administrators.
5. The issue of securing or locking the computer desktop shall remain the responsibility of the District. Any installation of security software or individual configurations of desktop policies will disrupt the efficiency of network administration and is prohibited.
6. System users may not use another person's system account without written permission from the campus administrator or District coordinator, as appropriate.
7. Use of non-district web-based email systems (such as Hotmail or Yahoo! Mail) is prohibited.
8. Students may not distribute personal information about themselves or others, nor shall any other system user distribute such personal information about others by means of the electronic communications system; this includes, but is not limited to, personal addresses and telephone numbers.
9. Students should never make appointments to meet people whom they meet on-line and should report to a teacher or administrator if they receive any request for such a meeting.
10. System users must purge electronic mail in accordance with established retention guidelines.
11. System users may not redistribute copyrighted programs or data except with the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with applicable copyright laws, District policy, and administrative regulations.
12. System users should avoid actions that are likely to increase the risk of introducing viruses to the system, such as opening e-mail messages from unknown senders and loading data from unprotected computers.
13. System users may not send or post messages that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
14. System users may not purposefully access materials that are abusive, obscene, pornographic, sexually oriented, threatening,

15. System users should be mindful that use of school-related electronic mail addresses might cause some recipients or other readers of that mail to assume they represent the District or school, whether or not that was the user's intention.
16. System users may not waste District resources related to the electronic communications system.
17. System users may not listen to or watch streaming media (music, videos, radio, and or television) over the network for personal use while at school. Streaming media places an undue burden on the district's network resources and is thus prohibited for personal use. Curriculum or business-related uses of streaming media are permitted.
18. System users should not forward any virus warnings of any kind to anyone other than the Technology Services Help Desk. Virus warnings that come from any other source than the Help Desk should be ignored.
19. Installation of personally purchased software on district computers is prohibited.
20. System users may not gain unauthorized access to resources or information. Deleting, examining, copying or modifying files/data that belong to someone else without permission is prohibited.
21. It is prohibited to leave your system unattended while logged on and not in use for any length of time. It is the user's responsibility to administer low-level security measures to protect against unauthorized use. Such measures might include a password-protecting screensaver or logging off and/or shutting down the computer. Users also have a responsibility to report security problems to the principal or network administrator.
22. Broadcast messages sent to all district staff must be approved by the appropriate central office administrator. Principals must approve broadcast messages within their own campus.

Intellectual
Property Rights

Any malicious attempt to harm or destroy District equipment or data or the data of another user of the District's system or of any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of District policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity 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, as well as other appropriate consequences. [See DH, FN series, FO series, and the Student Code of Conduct]

Disclaimer of
Liability

Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users, deliberate interference with the ability of other system users to send/receive electronic mail, or the use of another person's user ID and/or password is prohibited.

INFORMATION
CONTENT /
THIRD-PARTY
SUPPLIED
INFORMATION

System users and parents of students with access to the District's system should be aware that, despite the District's use of technology protection measures as required by law, use of the system may provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material.

A student who gains access to such material is expected to discontinue the access as quickly as possible and to report the incident to the supervising teacher.

A student knowingly bringing prohibited materials into the school's electronic environment will be subject to suspension of access and/or revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Student Code of Conduct.

An employee knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies. [See DH]

**EMPLOYEE AGREEMENT FOR ACCEPTABLE USE OF THE ELECTRONIC
COMMUNICATIONS SYSTEM**

Spring Branch Independent School District

Employee Application/Agreement for Network/Internet Account

Employee's Full Name: _____ **S.S.N.:** _____

School/Facility: _____ **Room/Office:** _____

Employee's Job Title: _____

I understand and will voluntarily abide by **Spring Branch Independent School District's Network/Internet Acceptable Use Guidelines**. I further understand that any violation of the guideline is unethical and may constitute a criminal offense. Should I commit such violations, my access privileges may be revoked. In addition, school disciplinary action and/or appropriate legal action may be taken. My signature indicates that I have read the **Spring Branch Independent School District's Network/Internet Acceptable Use Guidelines** carefully, understand its significance, and voluntarily agree to comply fully with all terms and conditions therein.

Date: _____ **Employee's Signature:** _____