

SBISD Electronic Communication and Data Management Guidelines

The Superintendent or designee will oversee the District's electronic communications system.

The District will provide training in proper use of the system and will provide all users with copies of acceptable use guidelines. All training in the use of the District's system will emphasize the ethical use of this resource.

CONSENT REQUIREMENTS

Copyrighted software or data may not be placed on any system connected to the District's system without permission from the holder of the copyright. Only the owner(s) or individual(s) the owner specifically authorizes may upload copyrighted material to the system.

No original work created by any District student will be posted on a web page under the District's control unless the District has received written consent from the student's guardian. [See [Exhibit A](#)]

No personally identifiable information about a District student will be posted on a web page under the District's control unless the District has received written consent from the student's parent. An exception may be made for "directory information" as allowed by the Family Education Records Privacy Act and District policy. [See [Exhibit A](#) and policies at [FL](#)]

SYSTEM ACCESS

Access to the District's electronic communications system will be governed as follows:

1. Students may be granted access to the District's system by their teachers, as appropriate.
2. The District suggests that all passwords be changed periodically.
3. 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.

DISTRICT RESPONSIBILITIES

The Superintendent 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 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 or on display. (See [Exhibit B](#), and [Exhibit C](#))
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 proper use of the system.
6. Set limits for data storage within the District's system, as needed.

SBISD Electronic Communication and Data Management Guidelines

INDIVIDUAL USER RESPONSIBILITIES

The user is being given access to the District's electronic communications system. Through this system, the user will be able to communicate with other schools, colleges, organizations, and people around the world through the Internet and other electronic information systems/networks. The user will have access to hundreds of databases, libraries, and computer services all over the world.

With this opportunity comes responsibility. It is important that the user read the District policy, administrative regulations, and agreement form and ask questions if help is needed in understanding them. Inappropriate system use will result in the loss of the privilege of using this educational and administrative tool.

Please note that the Internet is a network of many types of communication and information networks. It is possible that the user may run across some material the user might find objectionable. While the District will take reasonable steps to restrict access to such material, it is not possible to absolutely prevent such access. It will be the user's responsibility to follow the rules for appropriate use.

Rules For Appropriate Use

1. The account is to be used mainly for educational purposes, but some limited personal use is permitted as long as that personal use does not involve personal gain.
2. The individual in whose name a system account is issued will be responsible at all times for its proper use. Any generic accounts are the responsibility of the appropriate campus principal/department head and their designee
3. 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.
4. System users must purge electronic mail in accordance with established retention guidelines.

Inappropriate Uses

1. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy or guidelines.
2. Downloading or using copyrighted information without permission from the copyright holder.
3. System users may not use another person's system account without written permission from the campus administrator or District coordinator, as appropriate.
4. Students may not distribute personal information about themselves or others by means of the electronic communication system without the appropriate permission from the student's guardian. (See [Exhibit A](#))
5. 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.

SBISD Electronic Communication and Data Management Guidelines

6. System users may not install any software items without consent from appropriate administrative technology staff. System users are responsible for determining whether a program is in the public domain.
7. System users may not send or post messages that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
8. System users may not purposefully access materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
9. System users may not waste District resources related to the electronic communications system.
10. System users may not gain unauthorized access to resources or information.

Consequences For Inappropriate Use

1. Suspension of access to the system;
2. Revocation of the computer system account; or
3. Other disciplinary or legal action, in accordance with the District policies and applicable laws.

The user understands that his/her computer use is not private and that the District may monitor the user's activity on the computer system.

The user accepts the District's electronic communications system policy and administrative regulations and agrees to abide by their provisions. In consideration for the privilege of using the District's electronic communications system and in consideration for having access to the public networks, the user hereby releases the District, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from the user's use of, or inability to use, the system, including, without limitation, the type of damages identified in the District's policy and administrative regulations.

VANDALISM PROHIBITED

Any malicious attempt to harm or destroy District equipment or data or 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 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](#)]

FORGERY PROHIBITED

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.

SBISD Electronic Communication and Data Management Guidelines

INFORMATION CONTENT / THIRD-PARTY SUPPLIED INFORMATION

System users and parents of students with access to the District's system should be aware that 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. (See [Exhibit B](#) and [Exhibit C](#))

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](#)]

PARTICIPATION IN CHAT ROOMS AND NEWSGROUPS

Participation in chat rooms and newsgroups accessed on the Internet is permissible for students, under appropriate supervision, and for employees in accordance with District policies.

NETWORK ETIQUETTE

System users are expected to observe the following network etiquette:

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 are prohibited.
3. Pretending to be someone else when sending/receiving messages is considered inappropriate.
4. Transmitting obscene messages or pictures is prohibited.
5. Using the network in such a way that would disrupt the use of the network by other users is prohibited.

TERMINATION / REVOCATION OF SYSTEM USER ACCOUNT

Termination of an employee's or a student's access for violation of District policies or regulations will be effective on the date the principal or District coordinator receives notice of student withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

REQUIREMENTS FOR WEB PAGE PUBLICATION

A Web page is created under the auspices of the campus principal or administrative department head. A Web page can be created by any web page creation software or straight HTML. However, pages must reflect good coding practices and will NOT be published if they do not meet acceptable requirements by the Web Development Committee.

SBISD Electronic Communication and Data Management Guidelines

Examples:

1. The campus/department's web coordinator's name must be on file with the Web Development Team. This information may be emailed by the principal or department head to the [Director of Telecommunications](#).
2. The site folder/directory structure should be in alignment with the site's home page making the site easy to maintain by this year's web coordinator or next year's web coordinator.
3. When naming files or folders please avoid cryptic abbreviations so as to be understandable to anyone viewing the information.
4. Folder and file names should not contain capitals, spaces or slashes. Underscores are preferred for separation in names.
5. Unnecessary and excessive folders/directories will not be accepted. A folder should contain no less than 7-10 items.
6. Folders should be used to organize the site. Sites lacking needed folders will not be accepted.
7. A common graphics folder is acceptable for graphics used throughout the web site but for the most part, graphics and photos should be with the htm pages. This also facilitates transfer of web site ownership.
8. Pages with unnecessary coding will not be published.
9. For future pages and graphics, please keep file extensions to three letters - examples: .htm .jpg .gif .pdf

All photographs and work must be supported by proper consent forms. (See [Exhibit A](#)) A page is edited by a chosen editor (can be web coordinator or someone with editing skills) for grammar and spelling. The page is edited for content in keeping with SBISD web standards by the Campus Web Coordinator.

The page must be approved for content, spelling, & grammar by the campus principal, administrative department head or their designee. Principals and department heads are responsible for accuracy and appropriateness of information at the campus/department level.

The web page is then given to the [District Web Specialist](#) for publication. The web specialist will also proof both copy and code to be sure the pages are in keeping with district practices in regard to content, links, copyright adorns and code viability.

The [Executive Director of Communication](#) monitors all SBISD affiliate sites and reserves the right to remove inappropriate material.

Both the web coordinator and the principal/department head will be notified when the link is made to the Spring Branch web site.

SBISD Electronic Communication and Data Management Guidelines

CAMPUS WEB SITE CONTENT REQUIREMENTS

Each campus web site must contain the following information in an easily accessible portion of their site

1. SBISD identification
2. A link to the SBISD home page
3. A link to the SBISD employee e-mail search page
4. An indication of the last date updated
5. A link to the generic campus Email address (or designated account if preferred) for questions or concerns
6. A link to the SBISD copyright page
7. Campus Name
8. Campus Address
9. Campus Main Telephone and Fax Numbers
10. An email link to Building Principals and Main Contact points
11. Student Dress Code/Uniform information
12. Enrollment information (link back to district site for this)
13. Campus Calendars
14. District calendars (link back to district site for this)
15. Curriculum information (link back to district site for this)
16. Link to the Student/Performance Information page
17. Link to School Menus

SBISD Electronic Communication and Data Management Guidelines

DEPARTMENT WEB SITE CONTENT REQUIREMENTS

Each department web site must contain the following information in an easily accessible portion of their site

1. SBISD identification
2. A link to the SBISD home page
3. A link to the SBISD employee e-mail search page
4. An indication of the last date updated
5. A link to the generic department Email address (or a designated individual's account if preferred) for questions or concerns
6. A link to the SBISD copyright page
7. Department Name
8. Department Location and Physical Address
9. Department Telephone and Fax Numbers
10. Department Head and Main Contact points
11. Frequently Asked Questions and their answers
12. Forms provided by Department
13. Departmental Deadlines
14. Handbooks or Manuals

DISCLAIMER

The District's system is provided on an *as is, as available* basis. The District does not make any warranties, whether expressed or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. 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 user's requirements, or that the system will be uninterrupted or error free, or that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the system are those of the providers and not the District.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.