The Superintendent or designee will oversee the district's electronic communication 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 and safe 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 copyright owner, or an individual the owner specifically authorizes, may upload copyrighted material to the system.

No original work created by any district student or employee will be posted on a Web page under the district's control unless the district has received written consent from the student (and the student's parent if the student is a minor) or employee who created the work.

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 Educational Rights and Privacy Act and district policy.

Filtering

The Superintendent will appoint a designee to select, implement, and maintain appropriate technology for filtering Internet sites containing material considered inappropriate or harmful to minors. All Internet access will be filtered for minors and adults on computers with Internet access provided by the school.

The categories of material considered to be inappropriate and to which access will be blocked will include, but not be limited to: nudity/pornography, images or descriptions of sexual acts; promotion of violence, illegal use of weapons, drugs, discrimination, or participation in hate groups; instructions for performing criminal acts (e.g., bomb making); and on-line gambling.

Requests to Disable Filter

The designee will consider requests from users who wish to use a blocked site for bona fide research or other lawful purposes. Adjustments to the filter will be made where technically feasible.

System Access

Access to the district's electronic communications system (computer system and network) will be governed as follows:

Students in grades K-5 will be granted access to the district's system by campus/class as appropriate . In grades K-5 no student will be assigned an individual account or password.

Students in grades 6-12 will be assigned individual accounts.

1. As appropriate and with the approval of the immediate supervisor, district employees will be granted access to the district's system.
2. A teacher may apply for a class account and in doing so will be ultimately responsible for use of the account.
3. The district will require that all passwords be changed every year.
4. 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.
5. All users will be required to sign a user agreement and attend training annually for issuance or renewal of an account.

District and Technology Director Responsibilities

The technology director for the district's electronic communications system (computer system and network) 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 annually complete and sign an agreement to abide by district policies and administrative regulations regarding such use. All such agreements will be maintained and on file in the technology department.
3. Ensure that minors are provided training emphasizing the appropriate use of this resource, including appropriate online behavior, including interacting with other individuals on social networking Web sites and in chat rooms and cyber bullying awareness and response.
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 reconfigure a filtering device on the system for bona fide research or another lawful purpose.
7. Be authorized to establish a retention schedule for electronic messages on any electronic bulletin board and to remove messages posted locally that are deemed to be inappropriate.
8. Set limits for data storage within the district's system, as needed.

Individual User Responsibilities

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

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 purposes, in support of illegal activities 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 (computer system and network).
4. Communications may not be encrypted so as to avoid security review by system administrators.
5. System users may not use another person's system account without written permission from the campus administrator or technology director, as appropriate.
6. Students may not distribute personal information about themselves or others by means of the electronic communications system (computer system and network); this includes but is not limited to, personal addresses and telephone numbers.

7. 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.
8. Because emails and other computer files can be records, users are responsible for treating them as if they are paper records and retaining them according to the appropriate schedule. System users must purge electronic mail in accordance with the established retention guidelines. Emails and other digital communication on the district network are not routinely archived to storage media. Backup routines are strictly for disaster recovery purposes.
9. 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. Documentation must be presented to and kept on file with the technology department. Unlicensed material will be removed without notice.
10. 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.
11. System users may not download any program (whether shareware, freeware or commercial) to the system without approval from the technology department.
12. System users may not send or post messages that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
13. The distribution lists of the district's electronic mail system should not be used to generate unsolicited messages that do not communicate school business. This includes: forwarded jokes, forwarded inspirational messages, chain emails, emails from or about for-profit organizations or individuals seeking financial gain, and political advertising. The use of grade level and campus level email distribution lists is the responsibility of the campus or department administration. With the exception of illegal activity, violations of the acceptable use policy or any other unethical use, these lists are to be used at the discretion of the campus or department administrators. Anyone who wishes to address email to these lists must have consent or follow guidelines provided by the administrator of the campus for which those lists were created. Sending an email to a distribution list that includes members from more than one campus or department, such as the BCISD list, requires the approval of the sender's administrator.
14. System users may not purposefully access materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
15. System users should be mindful that the 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. System users should add the following disclaimer to all outgoing email messages: "This email contains the thoughts and opinions of [Employee Name] and does not represent official Burnet CISD policy."
16. System users may not waste district resources related to the electronic communications system (computer system and network). This includes but is not limited to unauthorized streaming of audio or video, transfer of large files, or any other bandwidth intensive activity unrelated to official school business. This also includes submitting your school issued electronic mail address to third parties for the purpose of receiving bulk electronic messages that are not related to school business.
17. System users may not gain unauthorized access to resources or information. This includes but is not limited to: attempting to "hack" into another computer system; obtaining a password or access to a system without explicit authorization; or using a computer that has been left signed-in but unattended.

18. Users shall not tamper with the computers, networks, printers, or other associated equipment except as directed by the computer technician.
19. Users may not connect non-district owned equipment to the district network or to computers that are connected to the district network without authorization from the Technology Department. The district purchases network software licenses based on the number of computers owned by the district. Antivirus software and network client licenses are necessary for the management of a safe and efficient network.

Vandalism Prohibited

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 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.

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 system (computer system and network)s 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 restriction, 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 the district policies. [See DH]

Participation in Chat Rooms, Social Networking Sites, Newsgroups and Use of Personal Email

Students are prohibited from participating in any web application that allows posting (chat, newsgroup, blogging site, personal email or social networking site) accessed on the Internet, unless the site has been approved by the district, and the student has been specifically instructed to do so for instructional purposes. Access of personal email accounts is permissible for employees, in accordance with district policies.

District Web Site

The district will maintain a district Web site for the purpose of informing employees, students, parents, and members of the community of district programs, policies, and practices. Requests for publication of information on the district Web site must be directed to the designated Webmaster. The technology director and the district Webmaster will establish guidelines for the development and format of Web pages controlled by the district.

No personally identifiable information regarding a student will be published on a Web site controlled by the district without written permission from the student's parent.

No commercial or political advertising will be permitted on a Web site controlled by the district.

School or Class Web Pages

Schools or classes may publish and link to the district's site Web pages that present information about the school or class activities, subject to approval from the Webmaster. The campus principal will designate the staff member responsible for managing the campus's Web page under the supervision of the district's Webmaster. Teachers will be responsible for compliance with district rules in maintaining their class Web pages. Any links from a school or class Web page to sites outside the district's computer system must receive approval from the district Webmaster.

Personal Web Pages

District employees, Trustees, and members of the public will not be permitted to publish personal Web pages using district resources.

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. Be considerate when sending attachments with e-mail by considering whether a file maybe too large to be accommodated by the recipient's system or may be in a format unreadable by the recipient.
6. Be considerate when choosing backgrounds and other stationery for email by considering that some of these are embedded images that consume resources on the recipient's computer.

Termination/Revocation of System User Account

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

The district's system is provided on an "as is, as available" basis. The district does not make any warranties, whether express 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 (computer system and network).

The district designates the following employee to receive any complaints that copyrighted material is improperly contained in the district Network:

Name: Connie Haines

Position: Technology Specialist

Telephone: 512-715-5119

E-mail: chaines@burnet.txed.net

Student Agreement for Acceptable Use of the Electronic Communications System (computer system and network)

You are being given access to the district's electronic communications system (computer system and network). You will have access to hundreds of databases libraries, and computer services all over the world. With this educational opportunity comes responsibility. It is important that you read the district policy, administrative regulations, and agreement form and ask questions if you need help in understanding them. Inappropriate system use will result in the loss of the privilege to use this educational tool. Please note that the Internet is a network of many types of communication and information networks. It is possible that you may run across areas of adult content and some material you (or your parents) might find objectionable. While the district will use filtering technology to restrict access to such material, it is not possible to absolutely prevent such access. It will be your responsibility to follow the rules for appropriate use.

Rules for Appropriate Use:

- Students in grades K-5 will have access through a campus/classroom student account. Students in grades 6-12 will be assigned and individual account. You are responsible for not sharing the password for your account with others.
- You will be held responsible at all times for the proper use of your account, and the district may suspend or revoke your access if you violate the rules.

Inappropriate Uses

- Using the system for any illegal purpose.
- Disabling or attempting to disable or bypass any Internet filtering device.
- Encrypting communications to avoid security review.
- Borrowing someone's account without permission from the technology department.
- Posting personal information about yourself or others (such as addresses and phone numbers).
- Downloading or using copyrighted information without the permission from the copyright holder and the technology department.
- Intentionally introducing a virus to the computer system.
- Posting messages or accessing materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
- Wasting school resources through the improper use of the computer system.
- Gaining unauthorized access to restricted information or resources.

Consequences for Inappropriate Uses

- Restricted or suspended access to the system;
- Vandalism will require restitution for costs associated with system restoration;
- Revocation of the computer system account; or
- Other disciplinary or legal action, in accordance with the Student Code of Conduct and applicable laws.

The student agreement must be renewed each academic year.

Student Name: _____

Grade: _____

School: _____

I understand that my computer use is not private and that the district will monitor my activity on the computer system. I have read the district's electronic communications system (computer system and network) policy and administrative regulations and agree to abide by their provisions. I understand that violation of these provisions may result in suspension or revocation of system access.

Student Signature: _____ **Date:** _____

Parent Name: _____

Home Address: _____

Home Phone Number: _____

_____ **I do not give permission for my child to participate in the district's electronic communications system (computer system and network)**

I have read the district's electronic communications system policy and administrative regulations. In consideration for the privilege of my child using the district's electronic communications system, and in consideration for having access to the public networks, hereby release the district, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my child's use of, or inability to use, the system, including, without limitation, the type of damage identified in the district's policy and administrative regulations.

_____ **I give permission for my child to participate in the district's electronic communications system and certify that the information contained on this form is correct.**

Parent Signature: _____ **Date:** _____