Dripping Springs
Independent School District
Operating Procedures

Index

ACCEPTABLE USE OF TECHNOLOGY

Electronic Communication & Data Management

The District's system will be used primarily for educational and administrative purposes consistent with the District's mission and goals. Commercial use of the District's system is prohibited. 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.

The District system (and other equipment) has a limited educational purpose. The purpose of the District system is to assist in preparing students for success in life and work in the 21st century by providing them with electronic access to a wide range of information and the ability to communicate with people from throughout the world. Additionally, the system will be used to increase District intracommunication, enhance productivity, and assist District employees in upgrading their skills through greater exchange of information with their peers. The District system will also assist the District in sharing information with the local community, including parents, social service agencies, government agencies, and businesses.

The term "educational purpose" includes use of the system for classroom activities, professional or career development, and limited high-quality self-discovery activities consistent with the mission and goals of the District.

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 and in accordance with the copyright/license of the software or data. Users who desire to use personal equipment or software must submit a Non-District Hardware/ Software Approval Form and secure approval of both campus and District technology staff. Personal software includes, but is not limited to, applications stored on personal flash drives and CD/DVD-ROM disks, as well as Internet applications.

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.

Personally identifiable information about a District student may be posted on Web pages maintained by the District only in accordance with the provisions below under "District Web Site".

Filtering

All Internet access will be filtered for minors and adults on computers with Internet access provided by the school. To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, the categories of material considered 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, drug use, discrimination, or participation in hate groups; instructions for performing criminal acts (e.g., bomb making); and on-line gambling. Users must not use proxy or "anonymous" sites or other measures to circumvent the filtering system.

Requests to Disable Filter

Requests from users who wish to use a blocked site for bona fide research or other lawful purposes may be considered.

System Access

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

1. Students will be granted access to the District's system as appropriate.
2. With a signed employee handbook receipt on file (which acknowledges the Acceptable Use Policy), District employees will be granted access to the District's system.
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.
4. The District's Acceptable Use Policy and Guidelines will govern all use of the District system. Student use of the system will also be governed by the Student Code of Conduct. Employee use will also be governed by District policy.
5. All users will be required to sign a user agreement as included in the Student Code of Conduct or the District Employee Handbook.

Campus-Level Supervisor Responsibilities

As the campus supervisor for the electronic communications system, the Principal or designee will:

1. Be responsible for disseminating and enforcing applicable District policies and acceptable use guidelines for the District's system and equipment at the campus level.
2. Serve as the building-level coordinator (campus supervisor) for the District system; approve building-level activities; ensure teachers receive proper training in the use of the system and the requirements of this policy; establish a system to ensure adequate

supervision of students using the system; maintain executed user agreements; and be responsible for interpreting the District Acceptable Use Policy at the building level.

3. Ensure that all users of the District's system complete and sign an acknowledgement of district policies and administrative regulations regarding such use. All such acknowledgements will be maintained on file in the Principal's office and may be included as part of the Student Handbook or campus handbook. Lack of a signed agreement does not indicate the right to disregard the policy or regulations.
4. Be authorized to monitor or examine all system activities, including electronic mail transmissions, as deemed appropriate to ensure proper use of the system.

District Level Responsibilities

The Technology Directors and Technology Instructional Coordinators for the District's electronic communications system (or campus designees) will:

1. Be responsible for disseminating, implementing, and enforcing applicable District policies and acceptable use guidelines for the District's system.
2. Carry out the daily operations of the district system and equipment, assist in the implementation of these guidelines and meet as necessary to advise and/or make recommendations to the superintendent, principals, and/or School Improvement Teams on the use of technology resources and systems.
3. Ensure that employees supervising students who use the District's system are provided 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.
7. Be authorized to establish a retention schedule for messages and files on any electronic system and to remove messages or files posted locally that are deemed to be inappropriate.
8. Establish a process for establishing individual and class accounts; set quotas for disk usage on the system; establish a retention schedule; establish a virus protection process; and perform other District-level activities.

Parental Notification and Responsibilities

1. The District will notify the parents about the District network and the policies governing its use. Parents may request alternate activities (that do not require Internet access) for their child(ren).

2. Parents have the right at any time to investigate the contents of their child(ren)'s e-mail files and other files. Parents have the right to request the termination of their child(ren)'s individual access at any time by contacting the school principal during school hours.
3. The District Acceptable Use Policy contains restrictions on accessing inappropriate material. There is a wide range of material available on the Internet, some of which may not be fitting with the particular values of the families of the students. It is not practically possible for the District to monitor and enforce a wide range of social values in student use of the Internet. Further, the District recognizes that parents bear primary responsibility for transmitting their particular set of family values to their children. The District will encourage parents to specify to their child(ren) what material is and is not acceptable for their child(ren) to access through the District system.

Individual User Responsibilities

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

1. The individual in whose name a system account or system access is issued will be responsible at all times for its proper use. Passwords are not to be shared.
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. Specifically, as required by the Children's Internet Protection Act, inappropriate usage includes (a) unauthorized access, including so-called "hacking" and other unlawful activities, and (b) unauthorized disclosure, use, and dissemination of personal information regarding minors.
3. System users may not disable, or attempt to disable, a filtering or security device or system.
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 District coordinator, as appropriate.
6. Except as provided under "Web Pages," students may not distribute personal information about themselves or others by means of the electronic communications system; this includes, but is not limited to, personal addresses and telephone numbers.
7. Students should never make arrangements to meet in person people whom they meet on-line, and should report to a teacher or administrator if they receive any request for such a meeting. Students will promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable.
8. System users must purge electronic mail in accordance with established retention guidelines.
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.

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 send or post messages that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

12. Inappropriate Language

    a. Restrictions against inappropriate language apply to public messages, private messages, and material posted on Web pages.

    b. Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.

    c. Users will not use ethnic or racial slurs.

    d. Users will not post information that, if acted upon, could cause damage or a danger of disruption.

    e. Users will not engage in personal attacks, including prejudicial or discriminatory attacks.

    f. Users will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending him or her messages, the user must stop.

    g. Users will not knowingly or recklessly post false or defamatory information about a person or organization.

13. System users may not purposefully access materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

14. Inappropriate Access to Material

    a. Users will not use the District system to access or transmit material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature). For students, a special exception may be made for hate literature if the purpose of such access is to conduct research and access is approved by both the teacher and the parent. Employees may access the above material only in the context of appropriate research.

    b. If a user inadvertently accesses such information, he or she should discontinue the access and immediately notify the supervising teacher, lab aide, or campus technology assistant. This will help protect users against an allegation that they have intentionally violated the Acceptable Use Policy.

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 must wisely use District resources related to the electronic communications system. Technology resources and access are provided for instructional purposes only. Users shall not use District equipment or systems for monetary gain or commercial purposes, defined as offering or providing goods or services. Purchasing goods or services for personal use is inappropriate. District acquisition policies will be followed for District purchase of goods or services through the District system. Users are not to incur any expenses to the District through the system without prior approval from the Technology Instructional Coordinator or Technology Director.

17. System users may not gain unauthorized access to resources or information.

18. Illegal Activities

    a. Users will not attempt to gain unauthorized access to the District system or to any other computer system through the District System, or go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of "browsing". Pretending to be someone else when sending/receiving messages is unacceptable.

    b. Users will not make deliberate attempts to disrupt the computer system performance or destroy data by spreading computer viruses or by any other means. These actions are illegal. Using the equipment in such a way that would disrupt the use of the equipment by other users is prohibited.

    c. Users will not use the District system to engage in any other illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of person, etc.

19. Users may not use the system for political lobbying, as defined by state statute. District employees and students may use the system to communicate with their elected representatives and to express their opinion on political issues.

20. In the case of any doubt about the acceptability of any specific use or operation of the system or equipment, users should contact their supervisor or technology coordinator for clarification.

21. System Security

    a. Users are responsible for the use of their individual account and should take all reasonable precautions to prevent others from being able to use their account. Users should not provide passwords to another person.

    b. Users will immediately notify their technology coordinator or campus supervisor if they have identified a possible security problem. Users will not go looking for security problems, as this may be construed as an illegal attempt to gain access.

    c. Users will avoid the inadvertent spread of computer viruses by following the District virus protection procedures

22. Plagiarism and Copyright Infringement

   a. Users will not plagiarize works that they find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.

   b. Users will respect the rights of copyright owners. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user should follow the expressed requirements. If the user is unsure whether or not they can use a work, he or she should request permission from the copyright owner.

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 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 may result in the cancellation of system use privileges and may require restitution for costs associated with system restoration, hardware, or software costs, as well as other appropriate consequences. [See District Handbook, 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 systems in the global electronic network that may contain inaccurate and/or objectionable material.

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 the District Handbook]

Search and Seizure

1. System users have a limited privacy expectation in the contents of their personal files on the District system.

2. Routine maintenance and monitoring of the system or files may lead to discovery that the user has violated or is violating the District Acceptable Use Policy, the Student Code of Conduct, or the law.
3. An individual search will be conducted if there is reasonable suspicion that a user has violated the law or the Student Code of Conduct. The nature of the investigation will be reasonable and in the context of the nature of the alleged violation.
4. District employees should be aware that their personal files may be discoverable under state public records laws.
5. Student-owned media are subject to interrogation and search as delineated in the Student Code of Conduct.

Copyright and Plagiarism

1. District policies on copyright will govern the use of material accessed through the District system. Because the extent of copyright protection of certain works found on the Internet is unclear, users should make a standard practice of requesting permission from the holder of the work if their use of the material has the potential of being considered an infringement. Teachers should instruct students to respect copyright, to request permission when appropriate, and use appropriate citation practices following Fair Use Guidelines.
2. District policies on plagiarism will govern use of material accessed through the District system.

Selection of Material

When using the Internet for class activities, teachers will select material that is appropriate in light of the age of the students and that is relevant to the course objectives. Teachers will preview the materials and sites they require or recommend students' access to determine the appropriateness of the material contained on or accessed through the site. Teachers will provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Teachers will assist their students in developing the skills to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.

District Web Site

The District will maintain a District Web site for the purpose of informing and communicating with employees, students, parents, and members of the community of District programs, policies, information, and practices. The Technology Directors and the District Webmaster will establish guidelines for the development and format of Web pages controlled by the District. No commercial advertising will be permitted on a Web site maintained by the District.

Web Pages

1. Names, student work, and photos of students may be placed on District Web pages as indicated on the District "Release of Directory Information" form.

2. Staff maintaining Web pages will be responsible for ensuring that student identification procedures are followed.

Personal Web Pages

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

Participation in Online Educational Activities

As one of many instructional tools, the Internet and other electronic resources may be used to enhance instruction. Parents and guardians have the right to exclude their child from Internet access by filing an Internet Denial Form.

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 Technology Director receives notice of student withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

Monitoring

As with all other school policies and guidelines, all staff share the responsibility of monitoring and guiding students in the appropriate use of technology. Failure to follow these guidelines may result in suspension or termination of privileges and other disciplinary action consistent with District policies and the Student Code of Conduct and District policy. Violations of law may result in criminal prosecution as well as disciplinary action by the District.

Disclaimer

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.