DRIPPING SPRINGS INDEPENDENT SCHOOL DISTRICT ACCEPTABLE USE OF TECHNOLOGY GUIDELINES - STAFF

Dripping Springs Independent School District's technology system and resources will be used primarily for educational and administrative purposes consistent with DSISD's vision, mission, and goals. Specifically, DSISD's system will be used to enhance and extend learning, facilitate communication, promote innovation, and provide tools for productivity.

DSISD expects employees to practice and model digital citizenship and to use district resources safely and ethically. The district Acceptable Use Policy [see Policy CQ] and Guidelines apply to use of district resources and job-related duties regardless of the location or equipment used.

Access to the System

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

- With a signed employee handbook (which acknowledges the Acceptable Use Policy and Guidelines) receipt on file, DSISD employees will be granted access to DSISD's system, as appropriate.
- DSISD's Acceptable Use Policy and Guidelines will govern all use of DSISD's system. Employee use will also be governed by other relevant district policy, Technology Operating Procedures, and the Employee Handbook.
- Users may connect personal equipment only to networks designated as BYOD networks. Users who wish to use personal software on DSISD devices must secure approval from a DSISD technology administrator.
- Any system user identified as a security risk or as having violated DSISD and/or campus technology use guidelines may be denied access to DSISD's system with or without notice.

Responsibilities - Supervisor

As the local supervisor for DSISD's system, the Principal, Director, or designee will:

- Enforce applicable DSISD policies and Acceptable Use Guidelines at the campus level and ensure that all users have a signed acknowledgement of the AUP and Guidelines.
- Ensure campus/department employees receive proper training in the use of the system and the requirements of the AUP and Guidelines. Lack of a signed agreement does not indicate the user's right to disregard the policy or guidelines.
- Be authorized to monitor or examine all system activities and data, including email transmissions, as deemed appropriate to ensure proper use of the system.

As the district-level supervisor, the Superintendent's designee(s) will:

- Disseminate, implement, and enforce applicable DSISD policies and Acceptable Use Guidelines.

- Carry out the daily operations of the DSISD system and equipment and advise and/or make recommendations on the use of technology resources and systems.
- Be authorized to monitor or examine all DSISD system activities and data, including email transmissions, as deemed appropriate to ensure safety and proper use of DSISD resources.
- Be authorized to disable a filtering device on DSISD's system for research or other lawful purpose.
- Be authorized to establish a retention schedule for messages and files on any DSISD electronic system and to remove messages or files posted locally that are deemed to be inappropriate.
- Be authorized to disable user access to DSISD's system upon a user's separation from DSISD or upon a user's violation of DSISD policies and guidelines.

Responsibilities – All Users

Access to DSISD's technology resources is a privilege, not a right. Noncompliance may result in suspension of access or termination of privileges and other disciplinary action consistent with DSISD policies. Violations of law may result in criminal prosecution, restitution of costs, and disciplinary action by DSISD.

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

- The system may not be used for or in support of illegal purposes or for any other activity prohibited by DSISD policy or guidelines. In particular,
    - Users will not attempt to gain unauthorized access to any DSISD system or to any other computer system through DSISD's system, or go beyond their authorized access. This activity includes attempting to log in through another person's account (even if the other person agrees) or to access another person's files.
    - Users will not impersonate someone else when sending/receiving email or other messages and will not interfere with the ability of others to send and receive messages.
    - Users will not make deliberate attempts to harm or destroy DSISD equipment or data or the data of another user within DSISD or of any agencies or other networks that are connected to the Internet or to degrade or disrupt system performance.
- Users may not circumvent, disable, or attempt to disable, a filtering or security device or system. This includes encrypting communications to avoid security review by system administrators through VPN and other applications.
- Inappropriate Language and Access to Material:
    - Users will not access or transmit:
        - Obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language or material.
        - Ethnic or racial slurs or material advocating violence or discrimination.
        - Language or material that, if acted upon, could cause damage or danger.
        - Language or material that advocates illegal acts.

    - Users will not engage in personal attacks, including prejudicial or discriminatory attacks and will not post false or defamatory information or material.
    - Users will not harass another person, engage in cyberbullying, or transmit material that may damage another's reputation. If a user is told by a person to stop sending him or her messages, the user must stop.
    - If a user inadvertently accesses inappropriate material, he or she should discontinue the access and immediately notify the supervising administrator or a technology staff member.
- Users must be mindful that use of DSISD-related electronic mail addresses might cause some recipients or other readers of that mail to assume they represent DSISD, whether or not that was the user's intention.
- Users must not use DSISD equipment or systems for personal monetary gain or commercial purposes.
- Users may not use the system for political lobbying, as defined by state statute. Users may use the system to communicate with their elected representatives and to express their opinion on political issues.
- Users are responsible for retaining (backing up) and purging electronic mail in accordance with established retention guidelines.
- System Security:
    - 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 (e.g., log out of devices and web applications each time). Users should not provide passwords to another person.
    - Users will immediately notify a technology administrator or campus supervisor if they have identified a possible security problem. Users will not search for security problems, as this action may be construed as an illegal attempt to gain access.
    - Users will avoid the inadvertent spread of computer viruses by following DSISD's virus protection procedures.
    - Employees must follow digital safety guidelines as published in the Technology Operating Procedures manual.
- Plagiarism and Copyright Infringement
    - 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 law, DSISD policy, and administrative regulations.
- Personally identifiable information about a DSISD student and student-created original work may be posted on web pages maintained by DSISD only in accordance with the provisions below under "District Website and Social Media."
- As with all other school policies and guidelines, all staff share the responsibility of monitoring and guiding students in the appropriate use of technology.

Privacy, Search, and Seizure

Users have a limited privacy expectation in the contents of their personal files on DSISD's system. Routine maintenance and monitoring of the system or files may lead to discovery that a user has violated or is violating the District Acceptable Use Policy and Guidelines, district policies and procedures, or the law. Additionally, an individual search will be conducted if there is reasonable suspicion that a user has violated the Acceptable Use Policy and Guidelines, district policies and procedures, or law. Furthermore, users should be aware that their personal files may be discoverable under state public records laws.

Selection of Material

When using the Internet or other electronic resources for class activities, instructional staff must

- select materials that are age-appropriate and relevant to learning objectives.
- preview all materials and sites to be used for instruction in order to determine appropriateness.
- consider CIPA, FERPA, PPRA, and COPPA requirements in the selection of material.
- provide guidelines to assist their students in selecting materials and channeling their activities effectively and properly.
- 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.

Prior to using or assigning the use of any software, subscription, or other resource requiring student accounts or student information, staff must follow the New Software Approval Process. Staff must not provide student accounts or student information to any site or app that has not been approved by DSISD per the approval process.

District Website and Social Media

DSISD will maintain a District website for the purpose of informing and communicating with employees, students, parents, and the community regarding DSISD news, programs, policies, practices, and other information. The Executive Director of Communications will establish guidelines for the development and format of web pages controlled by DSISD. Some general guidelines, however, are as follows:

- Names, student work, and photos of students may be placed on DSISD web pages and professional social media sites only as indicated on the annual DSISD Parental Objection form.
- Staff maintaining web pages and social media accounts will be responsible for ensuring that student identification procedures are followed to ensure that parents have permitted use of student information.
- No user will be permitted to publish personal webpages using District resources. Additionally, student names, work, and photos may not be placed on personal webpages or personal social media accounts.
- No commercial advertising will be permitted on a website maintained by DSISD without the approval of the Executive Director of Communications.

Termination / Revocation of System User Account or Access

Termination of a user's access for violation of DSISD policies or regulations or for separation from DSISD will be effective on the date the Principal or District Technology Director receives notice of revocation of system privileges or employee separation from employment, or on a future date if so specified in the notice. There is no requirement for DSISD to notify any user of account revocation, and the user should have no expectation of notification before or after access revocation.

Filtering/Third-Party Information/Disclaimer

To the extent practical, technology protection measures (or "Internet filters") shall be used to filter all Internet access and block inappropriate material. 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)
- online gambling

Users with access to DSISD's system should be aware that, despite DSISD'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. An employee knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with DSISD policies and guidelines.

DSISD's system is provided on an "as is, as available" basis. DSISD 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. DSISD 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 interrupted 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 DSISD.

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