Staff Acceptable Use Policy (AUP) [Regarding Students]

Posting Policies – Student Work, Pictures, Videos, Student Name - Technology

Denton ISD teachers or administrators may post the following with written parental/guardian and/or student approval to the principal:

- Student authored work
- Pictures, audio or video of student (alone or in a group)
- Student first and last names

Social Media Use with Students - Technology

- Read and follow all District policies.
- Read and follow the Terms of Use for all sites. For example, if the site says "you must be 13 to use this site," then it should not be used by students under 13
- Ensure that privacy settings protect students, faculty and the district.
- Do not share personally identifying information on education sites. (personal address, personal telephone number, personal pictures.)
- Instruct students in how to use the site for educational purposes
- Abide by AUP and Terms of Use for all Internet sites
- Report illegal, abusive, bullying, and other negative dangerous behaviors
- When setting up student accounts, do not use last names. Example: Use student's first name with the teacher's name. Example: Student Jenny in Ms. Taylor's class would use Jenny Taylor for name.
- Do not allow non-district users to participate on any classroom instructional site without administrative approval
- Invite administrator's access to the site being used
- Monitor student use of the site
- Delete all sites that are no longer in use

Electronic Communications Between Educators and Students

Allowed: The employee shall limit communications to matters within the scope of the employee's professional responsibilities (e.g., for classroom teachers, matters relating to class work, homework, and tests; for an employee with an extracurricular duty, matters relating to the extracurricular activity).

Prohibited: The employee is prohibited from knowingly communicating with students through a personal social network page; the employee must create a separate social network page ("professional page") for the purpose of communicating with students.

Hours Allowed: An employee may make public posts to an employee's social network site, blog, or similar application at any time.

Hours Prohibited: The employee shall not communicate directly with any student between the hours of midnight and 5:00 a.m.

Privacy / Retention / State & Federal Laws

- The employee does not have a right to privacy with respect to communications with students and parents.
- The employee continues to be subject to applicable state and federal laws, local policies, administrative regulations, and the Code of Ethics and Standard Practices for Texas Educators, including:
- Compliance with the Public Information Act and the Family Educational Rights and Privacy Act (FERPA), including retention and confidentiality of student records

Electronic Communications Between Educators and Students - Exemption

An employee is not subject to these provisions to the extent the employee has a social or family relationship with a student. For example, an employee may have a relationship with a niece or nephew, a student who is the child of an adult friend, a student who is a friend of the employee's child, or a member or participant in the same civic, social, recreational, or religious organization. An employee who claims an exception based on a social relationship shall provide written consent from the student's parent. The written consent shall include an acknowledgement by the parent that:

- The employee has provided the parent with a copy of this protocol
- The employee and the student have a social relationship outside of school;
- The parent understands that the employee's communications with the student are excepted from district regulation; and
- The parent is solely responsible for monitoring electronic communications between the employee and the student.

Electronic Communications Between Educators and Students - Definitions

The following definitions apply for the use of electronic media with students:

- **Electronic media** includes all forms of social media, such as text messaging, instant messaging, e-mail), Web logs/blogs, wikis, electronic forums/chat rooms, video-sharing Web sites, editorial comments posted on the Internet, and social network sites. Electronic media also includes all forms of telecommunication such as landlines, cell phones, and Web-based applications.
- **Communicate means** to convey information and includes a one-way communication as well as a dialogue between two or more people. A public communication by an employee that is not targeted at students (e.g., a posting on the employee's personal social network page or a blog) is not a communication: however, the employee may be subject to district regulations on personal electronic communications. Unsolicited contact from a student through electronic means is not a communication.

Electronic Communications Between Educators and Students - Parent's Request to Discontinue

Upon written request from a parent or student, the employee shall discontinue communicating with the student through e-mail, text messaging, instant messaging, or any other form of one-to-one communication.

Electronic Communications Between Educators and Students – Misconduct/Dismissal/Arrest

All employees are prohibited from soliciting or engaging in sexual conduct or a romantic relationship with a student.

Student Acceptable Use Policy (AUP)

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

Access to the District's electronic communications system, including the Internet, shall be made available to students and employees in accordance with administrative regulations. Access to the District's electronic communications system is a privilege, not a right.

All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the system and shall agree in writing to comply with such regulations and guidelines. Noncompliance with applicable regulations and guidelines may result in suspension or termination of privileges and other disciplinary action consistent with District Policies. [See DH, FNC, CQ, FO, and the Student Code of Conduct]

The Superintendent or designee shall develop and implement administrative regulations, guidelines, and user agreements, consistent with the purposes and mission of the District and with law and policy governing copyright. [See CQ]

Electronic mail transmissions and other use of the electronic communications system by students and employees shall not be considered confidential and may be monitored at any time by designated District staff.

The District shall not be liable for users' inappropriate use of electronic communication resources or violations of copyright restrictions, users' mistakes or negligence, or costs incurred by users. The District shall not be responsible for ensuring the accuracy or usability of any information found on the Internet.

Training

Denton ISD will provide training to users in proper use of the system and will provide all users with copies of the Denton ISD Acceptable Use Policy. All Denton ISD training for the system will emphasize its ethical use.

Copyrighted Materials

Copyrighted software of data may not be installed on the system without permission from the holder of the copyright. Only the owner of the copyright (or individuals the owner specifically authorizes in writing) may upload copyrighted material to the system.

Internet Safety

Denton ISD will use technology protection measures to prevent users and students from accessing pornography or other material deemed harmful to minors. Technology Protection Measures are defined as specific technologies that block or filter Internet access to inappropriate content. Inappropriate content is defined as:

- Obscene, as defined in section 1460 of title 18, United States Code.
- Child pornography, as defined in section 2256 of title 18, United States Code.

- Harmful to minors (including websites about violence, racism/hate).
- Disruptive to learning in the classroom (including sites with non-educational games).
- Inappropriate for minors (including websites that contain hacking instructions, Web email, Adware, Spyware, SPAM Internet fraud and scams and any other areas deemed inappropriate as determined by the campus administrator).
- Harmful to the technology protection measure (including websites with proxy servers that can be used to bypass the filters).
- Illegal (including piracy websites).
- Personal Web spaces should not identify the user's relationship to Denton ISD.
- Controls on the technology protection measures may be updated daily. Sometimes the controls may prevent access to sites needed for educational or administrative use. If a user needs to access a blocked site, they may submit a HEAT ticket to have the website reviewed.

Responsibilities

The Superintendent will designate a district-level administrator to:

- Disseminate and enforce acceptable use policies and guidelines at the district level.
- Ensure that all users read and sign an agreement to abide by Denton ISD's policies and guidelines regarding use of the system.
- Have campus personnel store student signed agreements (electronic or handwritten).
- Monitor activity on the system (as needed).
- Establish a retention schedule for messages on any electronic bulletin board. Remove local messages that are inappropriate.
- Set limits for disk utilization and mailbox sizes on Denton ISD's system.

Campus principals will designate campus-level coordinators to:

- Disseminate and enforce acceptable use policies and guidelines at the campus level.
- Ensure that teachers adequately supervise their students and are responsible for their students' use of the system.
- Ensure that teachers who supervise students provide training to students that emphasize appropriate use of the system.

Cyberbullying and Harassment

Threatening, harassing, and/or bullying others using electronic means to include the Internet and/or mobile technology is strictly prohibited.

Vandalism and Abuse

Vandalism is activity that intends to harm or destroy any part of the system, another user's data, or any agencies or network connected to the Internet or using any means to possess vandalism tools on network drives, pen drives, removable media, or the local computer.

Vandalism includes deliberate attempts to degrade or disrupt system performance. Vandalism includes, but is not limited to:

- Denials of Service (DOS) attacks
- Distributed Denial of Service (DDoS) attacks

- Uploading or creating viruses
- Using keystroke recording systems
- Loading Spyware or Adware
- Using port scanners or other tools to do network reconnaissance
- IP spoofing
- Man-in-the-Middle attacks
- Traffic sniffing
- Using any other tools to hack into or spy on the system

Vandalism is strictly prohibited and vandals will lose access to the system and must provide restitution for hardware and software costs associated with system restoration. Vandals may be prosecuted under applicable state and federal laws. Denton ISD will cooperate fully with local, state, or federal officials in any investigation concerning or relating to vandalism of Denton ISD's system, any other system or any investigation of misuse.

Email Abuse

Attempts to read, delete, copy, or modify the electronic mail of other users or deliberate interference with the ability of other system users to send/receive email is prohibited. Forgery or attempted forgery of email is prohibited.

Plagiarism

Copying any content from the Internet or the system that doesn't belong to the user and claiming that the content is the property of the user is prohibited. Users must cite the source when including content from the Internet or the system.

Third Party Content

Users and parents of students with access to the system should be aware that users and students might access other systems in the global network that may contain inaccurate and/or objectionable material. Any student or employee who brings prohibited materials into the system is subject to suspension, revocation of access, and is subject to disciplinary action in accordance with the Student Code of Conduct.

Revocation of Access

If any user violates the Acceptable Use Policy, Denton ISD may suspend the user's access to the system. Denton ISD will terminate the user's accounts on the date the campus principal or Denton ISD administrator receives notice of student withdrawal or revocation of system privileges, or on a future date if specified in the notice.

Disclaimers

System Access: Access to the system is provided on an "as is, available" basis. Denton ISD does not make any warranties with respect to any services provided by the system and about any information or software contained on the system. Denton ISD does not guarantee that the functions or services performed by, or that the information of software contained on the system will meet the user's requirements, or that the system will be uninterrupted or error-free, or that defects will be corrected.

User Information: Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the system belong to the providers and not Denton ISD.

Liability

Denton ISD is not liable for inappropriate use of Denton ISD’s system or violations of copyright restrictions, mistakes or negligence caused directly or indirectly by users, or costs that users incur. Denton ISD is not responsible for ensuring the accuracy or usability of any information on the Internet.