Dallas School District Acceptable Use Policy, AUP
Adopted from School District Policy IIBGA and Administrative Rule IIBGA-AR

General District Responsibilities

The district will:

1. Designate staff as necessary to ensure coordination and maintenance of the district's electronic communications system which includes all district computers, e-mail and Internet access;

2. Provide staff training in the appropriate use of the district's system including copies of district policy and administrative regulations. Staff will provide similar training to authorized system users;

3. Cooperate fully with local, state or federal officials in any investigation relating to misuse of the district's system;

4. Use only properly licensed software, audio or video media purchased by the district or approved for use by the district. The district will comply with the requirements of law regarding the use, reproduction and distribution of copyrighted works and with applicable provisions of use or license agreements;

5. Install and use desktop and/or server virus detection and removal software;

6. Provide technology protection measures that protect against Internet access by both adults and minors to visual depictions that are obscene, child pornography, or with respect to the use of computers by minors, harmful to minors. A supervisor or other individual authorized by the principal may disable the technology protection measures to enable access for bona fide research or other lawful purposes, as deemed appropriate;

7. Prohibit access by minors, as defined by CIPA and this regulation, to inappropriate matter on the Internet and World Wide Web;

8. Provide staff supervision to monitor the online activities of students to prevent unauthorized access, including “hacking” and other unlawful activities online, and ensure the safety and security of minors when authorized to use e-mail, chat rooms and other forms of direct electronic communication;

9. Provide student education about appropriate online behavior, including cyber bullying awareness and response, and how to interact with other individuals on social networking sites and in chat rooms;

10. Determine which users and sites accessible as part of the district's system are most applicable to the curricular needs of the district and may restrict user access, accordingly;

11. Determine which users will be provided access to the district's e-mail system;

12. Notify appropriate system users that:

    a. The district retains ownership and control of its computers, hardware, software and data at all times.
    b. Files and other information, including e-mail, sent or received, generated or stored on district servers are not private and may be subject to monitoring.
    c. The district may establish a retention schedule for the removal of e-mail;

d. E-mail sent or received by a Board member or employee in connection with the transaction of public business may be a public record and subject to state archivist rules for retention and destruction;
e. Information and data entered or stored on the district's computers and e-mail system may become discoverable evidence if a public records request is made or a lawsuit is filed against the district.
f. Passwords used on the district's system are the property of the district and must be provided to their supervisor or designated district personnel, as appropriate.
g. Transmission of any materials regarding political campaigns is prohibited.

13. Ensure all student and nonschool system users are informed of the district's electronic communications policy and administrative regulations. All such agreements will be maintained by the school office or as part of the student agenda. All students using Google Apps for Education must have a signed permission form.

14. Notify users of known copyright infringing activities and deny access to or remove the material.

System Access

1. Access to the district's system is authorized to:

   Board members, district employees, students in grades K-12, with parent approval and when under the direct supervision of staff, and district volunteers, district contractors or other members of the public as authorized by the system coordinator or district administrators consistent with the district's policy governing use of district equipment and materials.

2. Students, staff, Board members, volunteers, district contractors and other members of the public may be permitted to use the district's system for personal use, in addition to official district business, consistent with Board policy, general use prohibitions/guidelines/etiquette and other applicable provisions of this administrative regulation. Personal use of district-owned computers including Internet and e-mail access by employees is prohibited during the employee's on duty work hours. Additionally, Board member and employee use of district-owned computers may be permitted only when such use does not violate the provisions of ORS 244.040 and use is under the same terms and conditions that access is provided to the general public under the district's policy governing use of district equipment and materials.

General Use Prohibitions/Guidelines/Etiquette

Operation of the district's system relies upon the proper conduct and appropriate use by system users. Students, staff and others granted system access are responsible for adhering to the following prohibitions and guidelines which require legal, ethical and efficient utilization of the district's system.

1. Prohibitions

   The following conduct is strictly prohibited:

   a. Attempts to use the district's system for:

      (1) Unauthorized solicitation of funds;
      (2) Distribution of chain letters;
      (3) Unauthorized sale or purchase of merchandise and services;
      (4) Collection of signatures;

(5) Membership drives;
(6) Transmission of any materials regarding political campaigns.

b. Attempts to upload, download, use, reproduce or distribute information, data, software, or file share music, videos or other materials on the district's system in violation of copyright law or applicable provisions of use or license agreements;
c. Attempts to degrade, disrupt or vandalize the district's equipment, software, materials or data or those of any other user of the district's system or any of the agencies or other networks connected to the district's system;
d. Attempts to evade, change or exceed resource quotas or disk usage quotas;
e. Attempts to send, intentionally access or download any text file or picture or engage in any communication that includes material which may be interpreted as:

(1) Harmful to minors;
(2) Obscene or child pornography as defined by law or indecent, vulgar, profane or lewd as determined by the district;
(3) A product or service not permitted to minors by law;
(4) Harassment, intimidation, menacing, threatening or constitutes insulting or fighting words, the very expression of which injures or harasses others;
(5) A likelihood that, either because of its content or the manner of distribution, it will cause a material or substantial disruption of the proper and orderly operation of the school or school activity;
(6) Defamatory, libelous, reckless or maliciously false, potentially giving rise to civil liability, constituting or promoting discrimination, a criminal offense or otherwise violates any law, rule, regulation, Board policy and/or administrative regulation.

f. Attempts to gain unauthorized access to any service via the district's system which has a cost involved or attempts to incur other types of costs without specific approval. The user accessing such services will be responsible for these costs;
g. Attempts to post or publish personal student contact information unless authorized by the system coordinator or teacher and consistent with applicable Board policy pertaining to student directory information and personally identifiable information.
h. Attempts to arrange personal student meetings unless authorized by the system coordinator or teacher and with prior parent approval;
i. Attempts to use the district's name in external communication forums such as chat rooms without prior district authorization;
j. Attempts to use another individual's account name or password or to access restricted information, resources or networks to which the user has not been given access.
k. Attempts to connect any device including but not limited to personal laptops, desktop computers, printers, switched and wireless routers.

2. Guidelines/Etiquette

Appropriate system use etiquette is expected of all users and is explained in district training sessions.

Complaints

Complaints regarding use of the district's Electronic Communications System may be made to the teacher, principal, employee's supervisor or system coordinator. The district's established complaint procedure will be

used for complaints concerning violations of the district's Electronic Communications System policy and/or administrative regulation.

Violations/Consequences

1. Students

    a. Students who violate general system user prohibitions shall be subject to discipline up to and including expulsion and/or revocation of district system access up to and including permanent loss of privileges.
    b. Violations of law will be reported to law enforcement officials and may result in criminal or civil sanctions.
    c. Disciplinary action may be appealed by parents, students and/or a representative in accordance with established district procedures.

2. Staff

    a. Staff who violate general system user prohibitions shall be subject to discipline up to and including dismissal in accordance with Board policy, collective bargaining agreements and applicable provisions of law.
    b. Violations of law will be reported to law enforcement officials and may result in criminal or civil sanctions.
    c. Violations of applicable Teacher Standards and Practices Commission (TSPC), Standards for Competent and Ethical Performance of Oregon Educators will be reported to TSPC as provided by OAR 584-020-0041.
    d. Violations of ORS 244.040 will be reported to Oregon Governmental Ethics Commission.

3. Others

    a. Other guest users who violate general system user prohibitions shall be subject to suspension of system access up to and including permanent revocation of privileges.
    b. Violations of law will be reported to law enforcement officials or other agencies, as appropriate, and may result in criminal or civil sanctions.

Telephone/Membership/Data Access/Other Charges

1. The district assumes no responsibility or liability for any data access, membership, phone charges including, but not limited to, long distance charges, per minute (unit) surcharges and/or equipment or line costs incurred by any home usage of the district's system.

2. Any disputes or problems regarding data access or phone services for home users of the district's system are strictly between the system user and his/her local phone company and/or long distance service provider, or data access provider.

Information Content/Third Party Supplied Information

1. System users and parents of student system users are advised that use of the district's system may provide access to materials that may be considered objectionable and inconsistent with the district's mission and goals. Parents should be aware of the existence of such materials and monitor their student's home usage of the district's system accordingly.

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

3. System users who order services or merchandise through the district's system are solely responsible for all costs incurred as a result of such activity.

4. The district does not warrant that the functions or services performed by the system will be uninterrupted or error-free or that defects will be corrected or that the information or software contained on the system will meet the system user's requirements.