Dallas School District 2

Code: **IIBGA-AR**
Adopted: 10/14/02
Readopted: 11/24/04; 7/12/10; 7/12/12

# Electronic Communications System

**Definitions**

1. "Technology protection measure," as defined by the Children's Internet Protection Act (CIPA) means a specific technology that blocks or filters Internet access to visual depictions that are:

   a. Obscene, as that term is defined in Section 1460 of Title 18, United States Code;
   b. Child pornography, as that term is defined in Section 2256 of Title 18, United States Code; or
   c. Harmful to minors.

2. "Harmful to minors" as defined by CIPA means any picture, image, graphic image file or other visual depiction that:

   a. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex or excretion;
   b. Depicts, describes or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
   c. Taken as a whole, lacks serious literary, artistic, political or scientific value to minors.

3. "Sexual act; sexual contact" as defined by CIPA have the meanings given such terms in Section 2246 of Title 18, United States Code.

4. "Minor" as defined by CIPA means an individual who has not attained the age of 17. For the purposes of Board policy and this administrative regulation, minor will include all students enrolled in district schools.

5. "Inappropriate matter" as defined by the district means material that is inconsistent with general public education purposes, the district's mission and goals.

**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 cyberbullying 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. All communications and stored information transmitted, received or contained in the district's information system are the district's property and are to be used for authorized purposes only. Use of district equipment or software for unauthorized purposes is strictly prohibited. To maintain system integrity, monitor network etiquette and ensure that those authorized to use the district's system are in compliance with Board policy, administrative regulations and law, the school administrators may routinely review user files and communications;
    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. By using the district's system, individuals consent to have that use monitored by authorized district personnel. The district reserves the right to access and disclose, as appropriate, all information and data contained on district computers and district-owned e-mail system;
    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. "Deleted" or "purged" data from district computers or e-mail system may be retrieved for later public records disclosure or disciplinary purposes, as deemed necessary by 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. Passwords may be changed at the direction of the Superintendent or designee;
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 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. Personal student contact information includes photograph, age, home, school, work or e-mail addresses or phone numbers or other unauthorized disclosure, use and dissemination of personal information regarding students;
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, switches 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. All matters concerning merchandise and services ordered including, but not limited to, purchase terms, payment terms, warranties, guarantees and delivery are solely between the seller and the system user. The district makes no warranties or representation whatsoever with regard to any goods or services provided by the seller. District staff and administration shall not be a party to any such transaction or be liable for any costs or damages arising out of, either directly or indirectly, the actions or inactions of sellers.

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. 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.

**Dallas Internet Use, Student Email & Google Apps for Education Permission Form**

The District Acceptable Use Policy can be found here:
http://www.dallas.k12.or.us/pdf/AUP/Dallas%20AUP.pdf

It is important that you and your student read this permission form and discuss these requirements together. Inappropriate system use will result in discipline up to and including, suspension or revocation of your student's access to the district's system expulsion from school and/or referral to law enforcement officials. The following form must be signed as indicated. This form is available at your child's school, at the following link: http://goo.gl/Y95uG, or as a part of the student agenda. You may sign a paper form or submit your signature electronically at this link: http://goo.gl/oPYAv

Your school will provide students with Google Apps for Education (GAfE) which includes free, web based programs for Oregon students and teachers. This service is available through an agreement between Google and the State of Oregon. Apps for Education runs on an Internet domain purchased and owned by the school and is intended for educational use only.

GAfE is available at school and at home via the Internet. Email from known inappropriate sites is blocked, but there is always a chance students will be exposed to inappropriate content. School staff will monitor student use of Apps when students are at school. Parents are responsible for monitoring their child's use of GAfE when accessing programs from home. **Students are responsible for their own behavior at all times.**

**Child Internet Protection Act (CIPA)** – http://fcc.gov/cgb/consumerfacts/cipa.html
The school is required by CIPA to have technology measures and policies in place which protect students from harmful materials including obscene and pornographic. This means connections to the Internet are filtered and there are policies in place to protect students.

**Children's Online Privacy Protection Act (COPPA)** – http://www.ftc.gov/privacy/coppafaqs.shtm
COPPA applies to commercial companies and limits their ability to collect personal information from children under 13. Google advertising is turned off for GAfE users. No personal student information is collected for commercial purposes. This permission form allows the school to act as an agent for parents in the collection of information within the school context.

**Family Educational Rights and Privacy Act (FERPA)** – http://www2.ed.gov/policy/gen/guid/fpco/ferpa
FERPA protects the privacy of student education records and gives parents rights to review student records. Under FERPA, schools may disclose directory information but parents may request the school not disclose this information. Make this request to your school in writing.

1. The School will not publish confidential records (grades, student ID #, etc) publicly on the Internet.

2. The School may publish student work and photos for public viewing but will not publish other personally identifiable information.

3. Parents have the right at any time to investigate the contents of their student's email account and GAfE files.

GAfE are primarily for educational use. Students may use GAfE for personal use subject to the restrictions below and other school rules and policies which may apply.

1. Privacy – School staff, administrators and parents all have access to student email for monitoring purposes. **Students have no expectation of privacy with GAfE or on district systems.**

2. Limited personal use – Students may use GAfE for personal projects but may not use them for:

    a. Unlawful activities
    b. Commercial purposes or Personal financial gain (running a business or trying to make money)
    c. Inappropriate sexual or other offensive content
    d. Threatening another person
    e. Misrepresentation of Oregon Public Schools, staff or students. (Apps are extensions of classroom spaces where student free speech rights may be limited.)

3. Data Security – Student files and email are safe with GAfE but it is the responsibility of the student to make backups of important documents.

4. Safety

    a. Students may not post personal contact information about themselves or other people. This includes last names, addresses and phone numbers.
    b. Students will never agree to meet with someone they have met online without their parent's approval and participation.
    c. Students will tell their teacher or other school employee about any message they receive which is inappropriate or makes them feel uncomfortable.
    d. Students are responsible for the use of their individual accounts and should take all reasonable precautions to prevent others from accessing their account. Under no conditions should a user provide his or her password to another person.

5. Consumer safety (Advice for students and parents)

    a. Criminals create fake emails and web pages that look real. This is called phishing. Don't trust emailed links or web pages. Open a new browser window and search for the website yourself.
    b. Don't get spammed. Spam is unwanted advertising sent by email. Never reply to spam and never do business with a company that sends spam. Don't forward spam.

6. Digital Citizenship

    a. Treat others well. Be kind when using email or making a post on a forum or web page. Everyone will see what you write. Be careful with what you say about others and yourself.
    b. Respect the rights of copyright owners. Copyright infringement occurs when an individual inappropriately reproduces a work protected by a copyright. Works often contain language specifying acceptable use. Requirements should be followed.
    c. Your First Amendment rights to Free Speech can be limited in school. If you post something which disrupts the learning environment in your school, your right of speech may be limited. School web sites, email and groups are for educational use and are not considered public forums for debating ideas.

Access to and use of GAfE is considered a privilege accorded at the discretion of Dallas School District. The district maintains the right to withdraw the access and use of GAfE when there is reason to believe violations of law or district policies have occurred. In such cases, the alleged violation will be referred to the principal for further investigation and account restoration, suspension or termination. As a tenant of the Agreement with the State of Oregon, the state reserves the right to immediately suspend any user account in question of appropriate use. Pending review, a user account may be terminated as part of such action.

---

(detach and return to school)

Student Name: _____ Date: _____ Grade Year: _____

Parent/guardian:

I give permission for my child to use Google Apps for Education. By doing so I agree to enforce acceptable use when my child is off district property.

Parent signature: _____ Date: _____

**For students in fourth through twelfth grades**:

I have read the agreement above. I understand my Google Apps account will be monitored by school officials and I will be held accountable for my actions online.

Student signature: _____ Date: _____

**Agreement for an Electronic Communications System Account**
(Nonschool System User)

I have read the district's Electronic Communications System policy and administrative regulation and agree to abide by their provisions. I understand that violation of these provisions will result in suspension or revocation of system access and related privileges and/or referral to law enforcement officials.

In consideration for the privilege of using the district's Electronic Communications System and in consideration for having access to the public networks, I 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 use or inability to use the system including, without limitation, the type of damages identified in the district's policy and administrative regulation.

Signature: _____

Home Address: _____

Date: _____ Home Phone Number: _____