INFORMATION TECHNOLOGY

The Superintendent of Schools or designee (normally the head of the technology department) is charged with providing the technology environment to support the District's goals.

The Information and Technology Services Department (ITS) is responsible for design, development, implementation, and deployment of reliable technology and information systems, products, and services that support the educational infrastructure of the District.

Additionally, ITS is responsible for managing risks to the information systems and for collaborating with departments and campuses throughout the District to determine and implement controls that appropriately and proactively address the risks.

TECHNOLOGY GOVERNANCE COMMITTEE

The head of the technology department will establish and chair a Technology Governance Committee to facilitate the timely input, advice, policy proposals, implementation of projects, and information technology-related issues to influence the District's technology environment.

Agendas will be posted prior to each Technology Governance Committee meeting and meeting minutes will be posted after the meeting. As the committee chair, the Executive Director of ITS will be responsible for setting the agenda for each meeting.

The Technology Governance Committee is responsible for creating and maintaining the charter that establishes the mission statement, governance structure, and roles and responsibilities for technology governance in the District, which include but are not limited to the following:

1. Advise the Superintendent of Schools on the strategic technology direction for the District to ensure:
    a. IT policy development protects information assets and minimizes vulnerabilities;
    b. Project implementations meet the District's goals and objectives; and
    c. Governance of the IT infrastructure allows for adequate resources to maintain the District's information assets.
2. Recommend and advise on the security procedures and regulations relating to technology and security of information assets.
3. Approve technology projects.
4. Respond to issues, provide input, feedback, and advice to the administration and staff on concerns relating to technology.

5. Establish a standards sub-committee to create a baseline of District standards for hardware and software and monitor compliance after the baseline is established. This sub-committee will review new project and product requests for compliance with standards and will recommend any additions or changes to approved standards to the Technology Governance Committee.

6. Ensure that the technology policy and regulations are properly communicated throughout the District.

7. Establish a Technology Plan sub-committee to be responsible for developing a Technology Plan, based on input from campus staff, central departments, parents, students, and community members.

8. Develop and recommend to the Superintendent of Schools the Technology Plan.

9. Establish sub-committees as needed to govern major technology projects and initiatives.

10. Establish parameters for which technology projects and/or initiatives must be reviewed and approved by the Standards Sub-committee and/or the Technology Governance committee and communicate those processes to all affected stakeholders.

    The Technology Governance Committee may establish a Technology Advisory Council to solicit input on technology use, service quality, and initiatives from a broader group of individuals of varying roles and perspectives within the District.

    The Technology Governance Committee may sponsor various community outreach activities, including focus groups, forums, Webcasts, online discussion groups, a technology task force, and any other means necessary to obtain input and feedback on technology use, service quality, and initiatives.

DISTRICT PROPERTY

Unless third parties have clearly noted copyrights or some other rights including contract rights on the messages handled by these electronic communications systems, all messages generated on or handled by the District electronic communications systems are considered to be the property of the District.

NO PRIVACY EXPECTATIONS

Users have no expectation of privacy while using District technology resources.

INTENDED USE

In general, the District's computer and communication systems are intended to be used for business and educational purposes only

and are intended for use by employees, teachers, students, vendors, contractors, the community, and other third parties. Use of District technology and the District network requires that all users conduct themselves in a professional, responsible, decent, ethical, and polite manner at all times. Inappropriate system use or behavior will result in the loss of the privilege of using this educational and administrative tool and may result in disciplinary action including termination as well as civil or criminal penalties.

LIMITED PERSONAL USE

Limited use of the District's computing resources for personal purposes is permissible as long as the incremental cost of the usage is negligible, no District business activity is preempted by the personal use, and the usage is not likely to cause either a hostile working environment or a poor behavioral example.

The District's electronic communication systems must not be used for political advocacy efforts, religious efforts, private business activities, or personal amusement and entertainment. The District's electronic communication systems may be used for charitable fund-raising campaigns only with the express written permission of the Superintendent of Schools. News feeds, electronic mail mailing lists, push data updates, and other mechanisms for receiving information over the Internet must be restricted to material that is clearly related to both the District's business and the duties of the receiving users.

USE BY THIRD PARTIES

Use of the District's computer and communication systems by third parties must be authorized and third-party users must adhere to the same rules and regulations and controls deemed appropriate for employees, teachers, and students to ensure that sensitive information, assets, and resources are protected. Third parties must sign "acceptable use acknowledgements" for general use of the District's computing resources. They must also sign nondisclosure and confidentiality agreements before being granted authorized access to sensitive information.

ACCEPTABLE USE

The following regulations for acceptable and unacceptable use of computing devices using voice, video, and data networks, including the Internet, will apply to all District employees, teachers, students, vendors, contractors, and other third parties:

1. The District network, including the Internet, will be used primarily for instructional and administrative uses. This system will not be used for private gain, selling products or services, lobbying, or in violation of other law, policy, or regulation.

2. If the user identifies or knows of a security problem on the network, the user will notify a teacher or the site administrator. The teacher or the site administrator will then notify the Tech-

nical Assistance Center, who, depending on the severity of the problem, may notify Internal Audit. Except for notification, the user will not demonstrate and/or broadcast the security problem to other users.

3. Users must know the identity of the source of information and that it is a trusted source.

4. Users must use virus detection software prior to opening e-mails, documents, and other attachments.

5. Users will not install software on the District-supplied computers from the Internet or procured elsewhere without appropriate authority.

6. Users must confirm identity before releasing any internal District information, entering into any contracts, or ordering any products through public networks.

7. There should be signed contracts in place, and non-disclosure agreements for third parties and written agreements should be signed before any information is exchanged.

8. Spoofing, which is misrepresenting, obscuring, suppressing, or replacing a user's identity on the Internet or any District electronic communications system, is forbidden. The user name, electronic mail address, organizational affiliation, and related information included with messages or postings must reflect the actual originator of the messages or postings.

9. Users must not post unencrypted District material on any publicly accessible Internet computer that supports anonymous FTP or similar publicly accessible services, unless the posting of these materials has been approved by the director of public relations. The District's internal information must not be placed on any computer unless the persons who have access to that computer have a legitimate business need to know the involved information.

10. Use of "social networking" sites (MySpace, Facebook, LinkedIn, Blogging, Twitter, and the like) and blogging should adhere to the following:

    a. Limited and occasional use of the District's systems to engage in blogging is acceptable if authorized, provided that it is done in a professional and responsible manner, does not otherwise violate the District's policy, is not detrimental to the District's best interests, and does not interfere with an employee's regular work duties. The Dis-

trict reserves the right to block access to these or other Web sites.

b. Blogging by employees, whether using the District's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this regulation. Blogging from the District's systems is also subject to monitoring.

c. Users are also prohibited from discussing specific District business within any personal home pages they may have established on these sites outside of District business hours.

d. The District's Data Classification and Retention Regulation also applies to blogging. As such, employees are prohibited from revealing any District confidential or proprietary information, trade secrets, or any other material covered by the District's Data Classification and Retention Regulation when engaged in blogging.

e. Employees will not engage in any blogging that may harm or tarnish the image, reputation, and/or goodwill of the District and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory, or harassing comments when blogging or otherwise engaging in any conduct prohibited by the District's Nondiscrimination and Anti-Harassment policy.

f. Employees may also not attribute personal statements, opinions, or beliefs to the District when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent him or herself as an employee or representative of the District. Employees assume any and all risk associated with blogging.

g. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, the District's trademarks, logos, and any other District intellectual property may also not be used in connection with any blogging activity.

11. Users must not use the "save password" features on their Web browsers or electronic mail clients. The District's computer users must refuse all offers by software to place a cookie on their computer so that they can automatically log on the next time they visit a particular Internet site.

12. Users will not use or try to discover another user's password.

13. Users will not let other persons (other than authorized staff members) use their name, logon password, or files for any reason.

14. Users will not erase, rename, or make unusable another person's computer files, programs, or storage media.

15. Users will not copy, change, or transfer any software or documentation provided by the District, teachers, or students without authorization from the site administrator or designee.

16. Unauthorized access to the network, including so-called "hacking" and other unlawful activities, is prohibited. Such activities may include, but are not limited to:

    a. Writing, producing, generating, copying, propagating, or attempting to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer's memory, file system, or software;

    b. Intentionally damaging the system, including hardware and other associated equipment, damaging information belonging to others, misusing system resources, or allowing others to misuse system resources;

    c. Using unauthorized TCP/IP address assignments; and

    d. Implementing non-TCP/IP network communication protocols without authorization by the Technology Services Department.

17. Users will not access or create any obscene or objectionable information, language, or images. If such information is accessed accidentally, the user will immediately notify the site administrator or designee. The site administrator or designee will notify Network Services and will provide Network Services with the Web address of the site.

18. Users will not remove technology equipment (hardware or software) from District premises without written permission from the site administrator. The site administrator will keep such permission forms on file for a period of two years from the date of the authorization.

19. Users will not use the computers to transfer to others profane language, obscene images, or threats for the purpose of annoying or harassing others.

20. Users will not delete or change the electronic mail belonging to another system user or interfere with the ability of other system users to receive/send electronic mail without permission.

21. Unauthorized disclosure, use, and dissemination of personal information (e.g., picture, full name, home address, or home phone number, passwords or credit card numbers) regarding students, Board members, and employees of the District is prohibited. Users must never respond to unsolicited requests for personal information. Any such message should be immediately reported to the Information Security department. [See District intranet, inet.dallas-isd.org/forms]

22. Users will not defeat or make inoperative anti-virus software installed on District-owned workstations except temporarily for the expressed purpose of installing additional software when the anti-virus software interferes with the normal software installation.

ACCESS CONTROL

Access to information assets must be authorized, controlled, and monitored based upon job-related function and need-to-know criteria. [See CQ(EXHIBIT)-F] All information assets will be protected from unauthorized access, disclosure, duplication, modification, appropriation, destruction, loss, misuse, and denial of use.

PROTECTION

All District communications devices must be physically protected by locking in secured areas when not in use. All personal computer equipment must be marked with identification information that clearly indicates it is the District's property.

COPYRIGHTS

The reproduction, forwarding, or in any other way republishing or redistributing words, graphics, or other copyrighted materials must be done only with the permission of the author or owner. Users must assume that all materials on the Internet are copyrighted unless specific notice states otherwise.

Making unauthorized copies of licensed and copyrighted software, even if for "evaluation" purposes, is forbidden. The District permits reproduction of copyrighted materials only to the extent legally considered fair use or with the permission of the author or owner.

REPORTING SECURITY INCIDENTS

Users must promptly report all information security alerts, warnings, and suspected vulnerabilities to the Technical Assistance Center.

DAMAGED, LOST, OR STOLEN EQUIPMENT

Damaged, lost, or stolen equipment must be promptly reported to appropriate authorities and personnel.

USE OF PERSONAL EQUIPMENT	Use of non-District-owned technology equipment must meet a minimum set of security standards before connecting to the District's network. Users must adhere to the same rules and regulations and controls deemed appropriate for the District's networks. Those standards are established by the information and technology services department and appear in CQ(EXHIBIT)-E. Personal equipment is subject to the same monitoring and privacy expectations.
PROPERTY PASS	Computers, communication systems, and related information systems equipment must not leave the District's offices without proper authorization from the employee's supervisor/principal.
CHECKOUT OF HARDWARE AND SOFTWARE BY EMPLOYEES	Site administrators may permit District employees to take District-owned technology hardware and software home for use in conducting District business while at home. Such permission will be in written form. The site administrator will keep the forms on file for a period of two years from the date of the permission form. [See District intranet, inet.dallasisd.org/forms]
PERIODIC BACKUP	All sensitive, valuable, or critical information resident on the District's communication devices must be periodically backed up. All end users are responsible for making at least one current backup copy of sensitive, critical, or valuable files. Users should be mindful that the e-mail system is not backed up, and lost or deleted e-mail/information is not recoverable.
RECORD RETENTION	E-mail and other materials created on the District's network are subject to District and state record retention requirements.
DISPOSAL OF EQUIPMENT	The storage media of all technology equipment will be removed, destroyed, or purged prior to disposal or transfer of ownership outside the District.
UNAUTHORIZED NETWORK DEVICES	Neither District employees nor any other group will connect network devices not provided through, or approved by, the technology services department to the District network. Examples of such devices are: servers, routers, switches, hubs, wireless access points, and the like.
INAPPROPRIATE LANGUAGE	The use of inappropriate language in any electronic communication is prohibited, including the transmission and re-transmission of electronic mail containing illegal, profane, slanderous, libelous, defamatory, abusive, derogatory, threatening, obscene, racist, sexist, or otherwise offensive materials, harassment, and bullying.
TERMINATIONS	When employees, teachers, students, vendors, contractors, and other third parties are terminated from the District, all access to information assets will be promptly removed.

INTERNET SAFETY, ACCEPTABLE USE, AND SECURITY

All District employees will monitor the use of the District's network to ensure that the guidelines are followed. [See CQ(EXHIBIT)-A]

In order to ensure the safety and security of students, employees, and District information resources, access to e-mail, chat rooms, or other forms of direct electronic communications will only be available through Board-approved methods of electronic communication. Principals and department heads will be directly responsible for all e-mail, chat rooms, or other forms of direct electronic communications originating from the school/department to which the principal/department head is assigned. Being responsible entails taking appropriate and timely disciplinary action upon the principal or department head becoming aware of the unacceptable use of electronic communications by either students or employees. [See DH (LOCAL) and (REGULATION) regarding Personal Use of Electronic Equipment and Use of Electronic Equipment with Students]

STUDENT ACKNOWLEDGEMENT

Students will find the Acceptable Use Policy delineated in the Student Code of Conduct. The annual signing of the Student Code of Conduct agreement by a student or by a student's parent/guardian denotes acceptance of the Acceptable Use Policy. However, failure to sign the Student Code of Conduct agreement will not affect the applicability or application of the CQ(LOCAL) policy and this regulation. Any student who fails to comply with both the spirit and the letter of the Board policy [see CQ(LOCAL)] or its regulations may lose system privileges. Students may be disciplined in accordance with the Student Code of Conduct or other Board policies and District regulations governing student discipline. Students may also be the subject of appropriate legal action for violation of the policy in this code or its implementing regulations. [See CQ(EXHIBIT)-B and -C]

STUDENT E-MAIL ACCOUNTS

Student use of the District's e-mail communications require direct teacher supervision, parental consent, and the use of Children's Internet Protection Act (CIPA) solutions approved by the Technology Committee.

EMPLOYEE ACKNOWLEDGEMENT

Employees must sign an annual Acceptable Use Policy agreement before gaining access to the District's network. [See CQ(EXHIBIT)-D] Failure to sign the Acceptable Use Policy agreement will not affect the applicability or application of CQ(LOCAL) and this regulation. Any employee who fails to comply with both the spirit and the letter of this policy or its regulations may lose system privileges. Employees may also be subject to disciplinary action up to and including termination.

NO DEFAULT PROTECTION

Users using District computer and communication systems must realize that their communications are not automatically protected from viewing by third parties. Unless encryption is used, users

must not send information over the Internet if they consider it to be confidential or private.

MANAGEMENT REVIEW

At any time and without prior notice, the District's management reserves the right to examine electronic mail messages, files on personal computers, Web browser cache files, Web browser bookmarks, logs of Web sites visited, computer system configurations, and other information stored on or passing through the District's computers.

OFFENSIVE WEB SITES

The District is not responsible for the content that users may encounter when they use the Internet. Users using District computers who discover they have connected with a Web site that contains sexually explicit, racist, sexist, violent, or other potentially offensive material must immediately disconnect from that site and report to the Technical Assistance Center.

BLOCKING SITES AND CONTENT TYPES

The District may, at its discretion, restrict or block the downloading of certain file types that are likely to cause network service degradation. These file types include graphic and music files.

DEFINITIONS

The following definitions will apply:

- Blogging – Writing a blog. A blog (short for Weblog) is a personal online journal that is frequently updated and intended for general public consumption.
- Communications Devices - personal computers including laptops, notebooks, desktop workstations, and the like. Also handhelds, portables, personal digital assistants (PDAs), smart phones, and the like.
- Cyberbullying – Written/oral expression or physical conduct using the Internet:
    - That will have the effect of physically harming a student, damaging a student's property, or placing a student in reasonable fear of harm to the student's person or damage to the student's property; or
    - That is sufficiently severe, persistent, or pervasive to create an intimidating, threatening, or abusive educational environment for a student.
- Mobile Device – Portable cartridge/disk-based, removable storage media (e.g., floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain non-volatile memory) or portable computing and communications device with information storage capability (e.g., notebook/laptop computers, personal

digital assistants, cellular telephones, digital cameras, and audio recording devices).

- SPAMMING – Unauthorized and/or unsolicited electronic mass mailings.
- Third Parties – Include vendors, contractors, members of the public or community, and others doing business with the District and/or requiring use of the District's information assets.