TERRELL COUNTY BOARD POLICY **Descriptive Code: IFBG**
Internet Acceptable Use **Date: 2/13/2012**
Rescinds Code: IFBGA,CIPA
Date Issued: 6/10/1996, 11/14/2005

Introduction

The Board recognizes that as technologies shift the ways that information may be accessed, communicated and transferred by members of the society, those changes may also alter instruction and student learning. The Board generally supports access by students and staff to rich information resources. Telecommunications, electronic information sources and networked services significantly alter the information landscape for schools by opening classrooms to a broader array of resources. Telecommunications, because they may lead to any publicly available fileserver in the world, will open classrooms to electronic information resources which have not been screened by educators for use by students of various ages.

Electronic information research skills are now fundamental to preparation of citizens and future employees during an Age of Information. The Board expects that staff will blend thoughtful use of such information throughout the curriculum and that the staff will provide guidance and instruction to students in the appropriate use of such resources. Staff will establish classroom and media center guidelines for student use of network services; and closely supervise student use of the Internet/Intranet.

Students are responsible for good behavior on school computer networks. The network is provided for students to conduct research and communicate with others. Access to network services will be provided to students who agree to act in a considerate and responsible manner. Independent student use of telecommunications and electronic information resources will be permitted for instructional purposes. The guiding principles for the use of technological equipment are included in each school handbook for the students and parents or legal guardians of minor students (under 18 years of age).

It is the policy of Terrell County School System to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)]; and (e) provide instruction to students on the inherent dangers of social networking sites, the characteristics of cyberbullying and the recommended responses. School administrators will include cyberbullying in school bullying prevention plans, provide parents anti-cyberbullying information maintained on the district technology web page, and educate students about appropriate online behavior which includes interacting with other individuals on social networking websites and in chat rooms.

The Board authorizes the Superintendent to prepare appropriate procedures for implementing this policy and for reviewing and evaluating its effect on instruction and student achievement.

Responsibility of the District

It shall be the responsibility of all members of the District's schools and library staff to educate, supervise and monitor appropriate usage of the District's online computer network and access to the Internet.

In accordance with this policy, the Children's Internet Protection Act and the Protecting Children in the 21st Century Act, the District will teach Internet Safety to all students. This Internet Safety training will include cyber safety, cyber security and cyber ethics.

As a condition of Internet use at the District, each user must agree to comply with all applicable laws, rules, and regulations, including without limitation, all rules and regulations which may be established from time to time by the District. The District reserves the right to refuse access to the Internet to any person or persons for the violation of this or any other policy of the District, in accordance with applicable law.

Definitions

TECHNOLOGY PROTECTION MEASURE. The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:

1. OBSCENE, as that term is defined in section 1460 of title 18, United States Code;
2. CHILD PORNOGRAPHY, as that term is defined in section 2256 of title 18, United States Code; or
3. Harmful to minors.

HARMFUL TO MINORS. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
2. 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
3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

SEXUAL ACT; SEXUAL CONTACT. The terms "sexual act" and "sexual contact" have the meanings given such terms in section 2246 of title 18, United States Code.

Access to Inappropriate Material

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, and/or access to inappropriate information.

Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material

deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Acceptable Use

Operation of the network relies upon the proper conduct of the end users who must adhere to strict guidelines. Therefore, the use of the network must be in support of education and research consistent with the educational objectives of the Terrell County School System. Transmission of any material in violation of any United States or state regulation, or Terrell County School System's policy policies, is prohibited. This includes, but not limited to, copyrighted material, threatening, indecent, or obscene material or material protected by trade secret, use for commercial activities, product advertisement or political lobbying.

Unacceptable Use

The purpose of the Terrell County School System network is to support research and education. The Board reserves the right to determine the acceptability of any specific use of the network. The following guidelines, although not exclusive, constitute examples of unacceptable use of the Internet/Intranet:

1. No person shall use computers of the Terrell County School System for commercial business or profit or for solicitations of purchases of any kind.
2. Neither students nor employees will use network resources to play non-instructional computer games.
3. No person shall use any personal software without prior approval from the Technology Coordinator or the Network Support Manager.
4. No person shall deliberately access, remove, or copy any program or file on a computer belonging to someone else without specific authorization.
5. No person shall add, delete, copy programs, or tamper with existing programs in such a way that causes the computer to stop performing computer operations or that disrupts the use of the network by others.
6. No person shall engage in any conduct, including e-mail, chat rooms, or instant messaging, which harasses, libels, slanders, or in any way damages the reputation of another individual.
7. No person shall access, display, or send any materials that are profane, vulgar, threatening, pornographic, indecent, or harmful to minors.
8. No person may disguise or hide his/her identity, including changing his/her name on the system. Only members of the technology department may change any aspect of a user's account.
9. No person shall create "home pages" or directories without approval by the Technology Director.
10. Under no circumstances should students arrange to meet an individual they have contacted while using system-computing resources. Students should notify the classroom teacher and their parent or guardian immediately upon an attempt by any user to arrange to meet them or upon a contact from a user for an illicit or suspicious purpose.

The teacher, principal and Technology Director will have the discretion to immediately suspend or restrict any student or employee's access to and use of the Terrell County School System's network resources upon the apparent breach of these terms and conditions of acceptable use. Teachers and administrators may request suspension of another user's access rights upon notification of the Technology Director. The user will be informed of the suspected breach of the Acceptable Use Policy and given the opportunity to explain the situation. If this explanation is not satisfactory, the principal or the employee's supervisor will provide a written incident report to the Technology Director.

Supervision, Monitoring, and Privilege

The use of the Internet/Intranet is a privilege, and as such, is conditional upon the individual's compliance with any and all state and federal laws, school regulations, and the exercise of good manners. It shall be the responsibility of all members of the Terrell County School System staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet Protection Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Director of Network Services or designated representatives. Likewise, the Technology Director or Network Director may suspend or revoke privileges as deemed necessary.

Privacy

No student shall give out his/her personal information while using the Internet/Intranet resources of the Terrell County School System unless authorized and as required for participation in approved sites. In addition, information of this kind should not be given regarding any other user. No user shall give out his/her password to anyone other than the members of the Technology Department, nor shall any person use the account or password of any other Terrell County School System user. Breaches of privacy are direct violations of the Acceptable Use Policy.

It is not the intention of the Terrell County School system to actively monitor the electronic mail (e-mail) of account holders. However, there is no guarantee or reasonable expectation of privacy when e-mail is sent or received. During the course of maintaining the network, the members of the Technology Department will have access to all electronic messages and may inadvertently access inappropriate private messages or content that requires notification of the proper authorities. The Technology Director may be requested to access a user's e-mail by the Superintendent or other officials if inappropriate or harmful use of the network is suspected. It is the policy of the Terrell County School System that e-mail is not retained.

Security

Security of any computer system is a high priority. Any user who suspects or identifies a network security problem must notify a classroom teacher or building-level administrator

immediately. The principal or central office administrator should then notify the Technology Director. Network security problems must not be demonstrated to other users.

User passwords are one element of network security and should remain private. Users should not reveal their passwords or allow another person to use their password. Any individual who steals or attempts to steal another user's password will lose network privileges. Access rights are another level of network security. Any user who attempts to change the level of their his/her access rights or attempts to log into the network as a user with higher access rights will have their his/her network privileges immediately canceled and face disciplinary action. Any user identified as a security risk, or having a history of problems with other computer systems, may be denied access to the Terrell County School System's computer networks.

Copyright Guidelines

The Terrell County School System abides by all federal copyright guidelines, laws, and licensing agreements governing the use of software. All users must also abide by these guidelines. To avoid copyright infringements, individual users must not download software without the express prior permission of the Technology Director. Commercial software must be properly obtained and documented with official school system purchase orders. Single user software may not be installed on multiple machines and multi-station software must be installed in compliance with the number of users specified in the licensing agreement. Copyright infringement regarding commercial software must be reported to the Technology Director immediately. Employees may try "shareware" or "freeware" available on the Internet after approval by a member of the Technology Department. All conditions established by the authors of freeware and shareware must be followed, including payment after a trial evaluation period or limitations on the number of users. If there is a time limit on the use of the software, it must be removed in compliance with the author's wishes.

On the Internet, there are other forms of digital information (e.g. text, images, audio, sound, animations, etc.) that may also be affected by copyright laws. The creators of this information may claim such materials as their "intellectual" property. Users must avoid plagiarism (i.e. claiming the works of someone else as your own). Students or school system employees may not download on-line materials for use without complying with the conditions established by the creator (e.g. payment, acknowledgment, etc.). Users may capture such digital information (e.g. text, images, audio, sound, animations, etc.) for use in World Wide Web home pages, multimedia presentations, or school-related projects as long as copyright laws or a creator's specific restrictions are met. Copyright law generally allows the use of someone else's information for educational purposes but with the restriction that it cannot be sold nor publicly displayed. All questions and concerns about possible copyright violations of material obtained over the Internet must be directed to a school's Media Specialist or the Technology Director.

CIPA BACKGROUND

Full text of the Children's Internet Protection Act
http://www.fcc.gov/ccb/universal_service/chipact.doc

FCC regulations implementing CIPA; FCC 01-120
http://www.fcc.gov/Bureaus/Common_Carrier/Orders/2001/fcc01120.doc

SLD's FAQ on E-rate certification procedures and timing
http://www.sl.universalservice.org/reference/CIPAfaq.asp

Georgia Code Description Code
6-09-90 Georgia Computer Systems Protection Act
16-09-91 Computer Related Crime
16-09-92 Definitions
16-09-93 Computer crimes defined
16-09-93.1 Misleading transmittal
16-09-94 Violations

US Code
20 USC 6777 Internet Safety
47 USC 254(h) Universal Service
These references are not intended to be part of the policy itself, nor do they indicate the basis or authority for the board to enact this policy. Instead, they are provided as additional resources for those interested in the subject matter of the policy.