EAST GREENWICH TOWNSHIP SCHOOLS
ACCEPTABLE USE PROCEDURES

Guidelines:

The operation of the Internet relies heavily on the proper conduct of the users who must adhere to strict guidelines. **Internet access is a privilege, not a right**. If a district user violates any of the Acceptable Use provisions outlined in these procedures, his/her access will be terminated and future access will be denied.

Acceptable Use Procedures:

Acceptable Use Procedures for the Internet include, but are not limited to the following:

1) Use of the Internet must be in support of education and research, consistent with the educational objectives and curriculum of East Greenwich Township Schools.
2) Transmission of any materials in violation of U.S. or state regulations is prohibited.
3) Use of the Internet for religious or political messages is prohibited.
4) Use of the Internet to access, process, or transmit sexually explicit materials or information is prohibited.
5) Hate mail, harassment, discriminatory remarks or any other anti-social behavior is prohibited.
6) All illegal activities are prohibited.
7) Proper codes of conduct in electronic communication must be used. In news groups, giving out personal information is inappropriate. Students in grades K-6 will be granted access through classroom accounts when a teach requests said accounts for a particular classroom project. When using e-mail, extreme caution must always be taken in revealing any information of a personal nature.
8) Network accounts are to be used only by the authorized owner of the account for the authorized purpose.

Network Etiquette:

Teachers are expected to monitor the use of the Internet at all times and report misuse to the principal. Users are expected to abide by generally accepted rules of network etiquette. These include, but are not limited to the following:

1) Be polite. Do not get abusive in your messages to others.
2) Use appropriate language. Do not swear, use vulgarities, discriminatory remarks, ethnic slurs, or racial epithets.
3) Do not reveal your personal address or the telephone numbers and addresses of students or colleagues.
4) Our students will be communicating and collaborating with others both locally and globally via blogs, wikis, video conferencing, teacher generated email accounts, etc and must practice digital citizenship, cyber etiquette and cyber safety. Failure to do so may result in loss of technology privilege.

Security:

Security on any computer system is a high priority, especially when the system involves many users. All users have a vested interest in protecting the security of the system. Users have the responsibility of notifying the teacher or the building principal immediately of any potential security problem.

Vandalism:

Vandalism is defined as any malicious attempt to harm, destroy, or alter information of another user of the Internet or the school computer system. This includes, but is not limited to the uploading or creation of computer viruses. Vandalism will result in the cancellation of access privileges and possible disciplinary action.

Summary:

Appendix III-B2

The East Greenwich School District views information gathered from the Internet in the same manner as reference materials identified by the schools. Specifically, the district supports resources that will enhance the learning environment with guidance from the faculty and staff. Exploration and manipulation of resources is encouraged. However, it is impossible to control all materials on the global network. An industrious user may discover inappropriate information. The school district cannot prevent the possibility that some users may access material that is not consistent with the educational goals and policies of the school district.

Internet Safety Policy

Introduction

It is the policy of East Greenwich Township Schools 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)].

Definitions

Key terms are as defined in the Children's Internet Protection Act.

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, 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.

Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the East Greenwich Township Schools online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

East Greenwich Township Schools
Appendix III-B2

Supervision and Monitoring

It shall be the responsibility of all members of the East Greenwich Township Schools 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 district's technology coordinator or designated representatives.

Adoption

The Board of East Greenwich Township Schools adopted this Internet Safety Policy at a public meeting, following normal public notice, on April 28, 2010

CIPA definitions of terms:

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.

Appendix III_B2

EAST GREENWICH BOARD OF EDUCATION
Mickleton, New Jersey 08056

FILE CODE: 6142.10 {PRIVATE }
__X__ Monitored
__X__ Mandated
__X__ Other Reasons

Policy

TECHNOLOGY

The East Greenwich Board of Education shall develop a technology plan that effectively uses electronic communication to advance and promote learning and teaching. This system of technology shall be used to provide local, statewide, national and global communications opportunities for staff and students. Educational technology shall be infused into the district curriculum to maximize student achievement of the Core Curriculum Content Standards.

ACCEPTABLE USE OF THE INTERNET

Purpose

To support its commitment to providing avenues of access to the universe of information available, the district's system of electronic communication shall include access to the Internet for students and staff.

Limitation of Liability

The Internet constitutes an unregulated collection of resources that changes constantly, so it is not possible to totally predict or control the resources that users may locate. The board cannot guarantee the accuracy of the information or the appropriateness of materials that a user may encounter. Furthermore, the board shall not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. Nor shall the board be responsible for financial obligations arising through the unauthorized use of the system.

District Rights and Responsibilities

The computer system is the property of the district, and all computer software and hardware belong to it. Therefore, the district retains the right to monitor all access to and use of the Internet.

The board designates the Superintendent of Schools as the coordinator of the district system. He/she shall recommend to the board of education qualified staff persons to ensure provision of individual and class accounts necessary for access to the Internet, designation of quotas for disk usage on the system, establishment of a document retention schedule, establishment of a virus protection process and coordination of other activities as required to maintain the system.

Each principal shall coordinate the district system in his/her building by approving all activities for that building; ensuring that teachers receive proper training in the use of the system; ensuring that students are adequately supervised when using the system; maintaining executed user agreements; and interpreting this acceptable use policy at the building level.

TECHNOLOGY (continued)

Access to the System

This acceptable use policy shall govern all use of the system. Sanctions for student misuse of the system shall be included in the disciplinary code for students, as set out in regulations for policy 5131 Conduct/discipline. Employee misuse may result in appropriate discipline in accord with the collective bargaining agreement and applicable laws and regulations.

The board shall ensure the acquisition and installation of blocking/filtering software to deny access to certain areas of the Internet.

World Wide Web

All students and employees of the board shall have access to the Web through the district's networked or stand alone computers. An agreement may be required. To deny a child access, parents/guardians must notify the building principal in writing.

Classroom E-mail Accounts

Students in grades K-6 shall be granted e-mail access through classroom accounts only. To deny a child access to a classroom account, parents/guardians must notify the building principal in writing.

Individual E-mail Accounts for Students

Students in grades K-6 may have individual accounts at the request of teachers and with the consent of parents/guardians. An individual account for any such student shall require an agreement signed by the student and his/her parent/guardian.

Individual E-mail Accounts for District Employees

District employees shall be provided with an individual account and access to the system. An agreement may be required.

Supervision of Students

Student use of the Internet shall be supervised by qualified staff.

District Web Site

The board authorizes the Superintendent of Schools to establish and maintain a district web site. The purpose of the web site will be to inform the district educational community of district programs, policies and practices.

Individual schools and classes may also establish web sites that include information on the activities of that school or class. The building principal shall oversee these web sites.

The Superintendent of Schools shall publish and disseminate guidelines on acceptable material for these web sites. The Superintendent of Schools shall also ensure that district and school web sites do not disclose personally identifiable information about students without prior written consent from parents/guardians. Consent shall be obtained on the form developed by the state department of education. "Personally identifiable information" refers to student names, photos, addresses, e-mail addresses, phone numbers and locations and times of class trips.

Parental Notification and Responsibility

The Superintendent of Schools shall ensure that parents/guardians are notified about the district network and the rules governing its use. Parents/guardians shall sign an agreement to allow their child(ren) to have an individual account. Parents/guardians who do not wish their child(ren) to have access to the Internet must notify the principal in writing.

Acceptable Use

Student Safety Practices

Students shall not post personal contact information about themselves or others. Nor shall students engage in any kind of personal contact with individuals they meet online. Attempts at contact from such individuals shall be reported immediately to the staff person monitoring that child's access to the Internet. Personal contact information includes but is not limited to names, home/school/work addresses, telephone numbers, or personal photographs.

Prohibited Activities

Users shall not attempt to gain unauthorized access to the district system or to any other computer system through the district system, nor shall they go beyond their authorized access. This includes attempting to log in through another individual's account or accessing another's files.

Users shall not deliberately attempt to disrupt the district's computer system performance or destroy data by spreading computer viruses, worms, "Trojan Horses," trap door program codes or any similar product that can damage computer systems, firewalls, servers or network systems.

Users shall not use the district system to engage in illegal activities.

Users shall not access material that is profane or obscene, that advocates illegal acts, or that advocates violence or hate. Inadvertent access to such material should be reported immediately to the supervising staff person.

Users shall not plagiarize material that is available on the Internet. Plagiarism is presenting another's ideas/words as one's own.

Users shall not infringe on copyrighted material and shall follow all dictates of copyright law and the applicable policies of this district.

TECHNOLOGY (continued)

Prohibited Language

Prohibited language applies to public messages, private messages, and material posted on web pages.

Users shall not send or receive messages that contain obscene, profane, lewd, vulgar, rude, inflammatory, or threatening language.

Users shall not use the system to spread messages that can reasonably be interpreted as harassing, discriminatory or defamatory.

System Security

Users are responsible for their accounts and should take all reasonable precautions to prevent unauthorized access to them. In no case should a user provide his/her password to another individual.

Users shall immediately notify the supervising staff person or data processing department if they detect a possible security problem. Users shall not access the system solely for the purpose of searching for security problems.

Users shall not install or download software or other applications without permission of the supervising staff person.

Users shall follow all district virus protection procedures when installing or downloading approved software.

System Limits

Users shall access the system only for educational, professional or career development activities. This applies to discussion group mail lists, instant message services and participation in Internet “chat room” conversations.

Users shall check e-mail frequently and delete messages promptly.

Privacy Rights

Users shall respect the privacy of messages that they receive and refrain from reposting messages without the approval of the sender.

Users shall not publish private information about another individual.

Implementation

The Superintendent of Schools shall prepare regulations to implement this policy.

TECHNOLOGY (continued)

NJSBA Review/Update: December 2009
Adopted:

Key Words

Acceptable Use, Blocking/Filtering Software, E-mail, Internet, Technology, Web Site, World Wide Web

Legal References:

N.J.S.A. 2A:38A-1 et seq.	Computer System
N.J.S.A. 2C:20-25	Computer Related Theft
N.J.S.A. 18A:7A-11	Annual report of local school district; contents; annual report of commissioner; report on improvement of basic skills
N.J.S.A. 18A:36-35	School Internet websites; disclosure of certain student information prohibited
N.J.A.C. 6A:30-1.1et seq.	Evaluation of the Performance of School Districts
17 U.S.C. 101	United States Copyright Law
47 U.S.C. 254(h)	Children's Internet Protection Act
N.J. v. T.L.O. 469 U.S. 325 (1985)	
O'Connor v. Ortega 480 U.S. 709 (1987)	
No Child Left Behind Act of 2001, Pub. L. 107-110, 20 U.S.C.A. 6301 et seq.	

Possible Cross References:

*1111	District publications
*3514	Equipment
3543	Office services
*3570	District records and reports
4118.2/4218.2	Freedom of speech (staff)
*5114	Suspension and expulsion
*5124	Reporting to parents/guardians
*5131	Conduct/discipline
*5131.5	Vandalism/violence
*5142	Pupil safety
5145.2	Freedom of speech/expression (students)

TECHNOLOGY (continued)

*6144	Controversial issues
*6145.3	Publications
6161	Equipment, books and materials

*Indicates policy is included in the Critical Policy Reference Manual.