

Greeneville City Schools

Procedures and Guidelines

ACCEPTABLE USE, MEDIA RELEASE, AND INTERNET

SAFETY PROCEDURES

Page 1 of 4

PURPOSE

The Greeneville City Schools provides students and employee access to the Internet as a means to increase learning and productivity toward achieving 21st century literacy. The purpose of this contract is to ensure that users recognize the procedures which the school imposes on their use of Internet, electronic media resources, and release of student information. In addition, this contract requires that users agree to abide by the Greeneville City Schools Board of Education policies, the Greeneville City Schools Computer Guidelines, and stipulations of the Children's Online Protection Act 47 USC Section 231 (COPPA), the Family Education Rights and Privacy Act (FERPA), and the Children's Internet Protection Act (CIPA) as well as Laws pertaining to stalking and harassment. The policy is promulgated so as to be in compliance with the public records laws of the State of Tennessee.

THE CONTRACT

The Greeneville City Schools has outlined the following guidelines as required for all technology users. The district has taken measures designed to protect students and adults from obscene information and restrict access to materials that are harmful to minors. Failure to follow all or part of these guidelines, or any action that may expose the Greeneville City Schools to risks of unauthorized access to data, disclosure of information, legal liability, potential system failure, or compromise the safety of users is prohibited and may result in disciplinary action up to and including loss of network privileges, confiscation of computer equipment, suspension, termination of employment and/or criminal prosecution.

1. Employee Compliance

All employees must comply with all Greeneville City Board of Education policies, Greeneville City Schools Web Publishing Guidelines, and the Greeneville City Schools Computer Guidelines.

2. Student Compliance

Users shall not attempt to make use of material or attempt to locate material which would not be acceptable in a school setting. Students will be supervised by faculty during use of online resources. All students must comply with all Greeneville City Board of Education policies and the Greeneville City Schools Computer Guidelines.

Students shall report to school personnel any electronically transmitted attacks in any form made by others over the Internet or local network using any Greeneville City Schools' technology. Students shall understand information obtained via the Internet may or may not be correct.

3. Internet Safety

All students will participate in Internet safety instruction integrated into the district's instructional program in grades K-12.

Internet safety professional development is available to all teachers and administrators through the district provided Internet safety on-line courses and other professional development activities.

Outreach programs to families and community are offered annually. Schools will use existing avenues of communication to inform parents about Internet safety. The district Internet safety policy is reviewed annually.

4. Network Security

Only users with valid Greeneville City School network accounts are authorized to use the Greeneville City School's network and computer equipment. Employees and students must only use their assigned network account. Users are prohibited from giving anyone your network password or network account information other than to authorized personnel.

Do not allow anyone to use a computer while you are logged in. All computer users should always logoff from the network before leaving their room or office.

For the protection and security of Greeneville City Schools data, all computers attached to the Greeneville City Schools physical network (a computer located at a Greeneville City Schools facility either wired or wireless), must be the property of Greeneville City Schools. It is prohibited to attach a computer that is not property of Greeneville City Schools to the network without first receiving approval from IT Department management.

Use of software designed to gain passwords or access beyond the rights assigned to a user or computer are strictly prohibited. Use of such programs risk the security of the network and is considered "hacking". The intent to control unauthorized access is a violation of State and Federal law. Violators will be prosecuted. Should you inadvertently discover passwords or any other measure used to control unauthorized access, you must report your discovery to supervisory personnel in the room (in the case of students) or IT personnel (in the case of staff).

No user shall encrypt files or folders or attempt to hide files or folders stored on a network server or local workstation. Any encrypted or hidden files will be archived for further review and then deleted upon discovery with no warning. Our staff will log that you have hidden/encrypted files. Further action may result.

All network users may be monitored at any time by authorized personnel for the purpose and inspection of compliance to these guidelines.

5. Workstation/Computer Use

All employees and students are prohibited from installing any software on any computer unless authorized in writing by a member of the IT Department. Illegal downloads or use of copyrighted software, music, videos, pictures or other files is strictly prohibited.

All employees and students are prohibited from using any computer for illegal or commercial activity.

Any desktop applications designed to limit access to students or staff, other than those used by the IT Department for network security purposes, is prohibited.

Changing or tampering with any computer's system configuration is strictly prohibited.

Use of any broadcast messenger service such as "net send" to send messages over the network is prohibited except in the case of an emergency.

Installing and using personal accounts is prohibited under all circumstances through any type of access or connectivity to include private phone lines.

No desktop computer shall be moved by anyone other than IT Department personnel unless approved by a member of the IT Department.

6. Server Software

Only authorized IT Department personnel will install software to the server.

7. Saving Documents

Employees and students must save all documents to the network. Do not save any applications to the network, only documents and data. Due to server storage limitations, any applications or executables residing in your user directory will be deleted. (Exception is given where individuals have created applications as part of a curriculum assignment and such activity has been approved by a member of the Greeneville City Schools' faculty or staff.) Any documents residing solely on your local computer are at risk. It is your responsibility to make sure important documents and data are saved to the network. All personal files on your computer(s) are solely your responsibility. This includes, but is not limited to: stored passwords, pictures, documents, or applications. In the event of a reload of the machine, either intentional or inadvertent, any locally stored data may be irretrievably lost. You are strongly encouraged to make and maintain regular backups of any data you choose not to store on your I: drive. If you need assistance in learning how to backup personal files, or how to keep them on removable media, please work with your building technology leader.

8. Viruses and Virus Protection

The Greeneville City School's IT Department will provide all virus protection and related software for all workstations and servers. Virus protection and related software will be installed by authorized IT personnel unless otherwise approved by the IT Department.

Do not open any e-mail attachments from anyone you do not know. Never send anyone an e-mail you suspect may contain a virus. The intentional spreading of messages or files containing damaging or destructive programs or data is against federal law. Violators will be prosecuted. If you feel your computer may contain a virus, please contact the IT Department immediately.

There are many virus hoaxes. Never delete system files from a computer in order to remove a potential virus without first checking with the IT Department to make sure the virus is valid and not a hoax. Never forward reported virus warnings without first checking with the IT Department to make sure the virus is valid and not a hoax, unless they originated from the Greeneville City Schools IT staff.

9. Copyright Policy

All students and employees will comply with all applicable copyright laws in the use of all media and materials. All employees will model legal and ethical practice related to technology use as established in Greeneville City Board of Education policies.

10. E-mail

The Greeneville City Schools e-mail system has been provided for the internal and external communication of employees and board members. Responsible and ethical use of the e-mail system is required. The e-mail system may not be used for personal gain, or political or religious views or in any illegal, offensive or unethical manner. The e-mail system is intended only for valid and legitimate Greeneville City Schools' related communication.

Greeneville City Schools does reserve the right to access any e-mail for any business purpose, and also for inspection for disciplinary or legal actions. Your email may be accessed with or without your knowledge. Deleting messages from your message store will not prevent our staff from viewing all mail sent to or from your account.

All email is archived for regulatory compliance and potential further review. The end user is not able to circumvent the mail archive.

All email is filtered for content. Email containing offensive words or themes will not be delivered. Our IT staff may contact the sender, the recipient, or both; in addition to any other relevant authorities. All video files are stopped entering and leaving our network for review by our staff.

No email message may be larger than 10 megabytes (mb).

Students may be issued an e-mail account for the purpose of completing school work. Accounts may include access to chat and message boards within the educational system. Student e-mail accounts are filtered for content and monitored by authorized personnel. Students are not allowed to use the account to communicate outside of the educational

system. Students must use appropriate language in all communications. The use of profanity, obscenity, and offensive or inflammatory language is strictly prohibited and will result in disciplinary action. Instruction on safe and appropriate use will accompany the issuance of accounts.

11. Donations

The current standard for donated computers is a Pentium 4, 1.1 GHz or above CPU, with a 40 GB hard drive and 512 MB RAM.

Greeneville City Schools reserves the right to modify these guidelines as deemed necessary in order to provide a safe and secure environment for the technological needs of employees, students and board members. We appreciate your cooperation in following these guidelines.

Greeneville City Board of Education Procedures and Guidelines

ACCEPTABLE USE, MEDIA RELEASE, AND INTERNET

SAFETY PROCEDURES

ACCEPTANCE OF TERMS AND CONDITIONS:

These terms and conditions reflect the entire agreement of the parties and supersede all prior oral and written agreements and understandings of the parties.

If you are under the age of 18, a parent or guardian must also read and sign this contract.

I understand that should I fail to honor all the terms of this contract, future Internet and other electronic media accessibility may be denied, and the school administration will consider it a major disciplinary offense.

Student Name (Please Print) _____

Student Signature _____

Date _____

I have read this contract and understand that the school wishes to expand the availability of information to students and at the same time attempt to assure the appropriateness of this information as it relates to the goals of the school. By signing below, I give permission for the school to allow my son or daughter to have access to the Internet and other technology resources under the conditions set forth above.

Parent or Guardian Name (Please Print) _____

Parent or Guardian Signature _____

Date _____

I agree to the following release of information regarding my child:

The school or school district may feature students in the local broadcast and print media, on the school or school district web site, and in district publications and programs. If you do not want your child to be included in these activities, please provide written notification to your student's principal.

Greeneville City Board of Education Procedures and Guidelines

ACCEPTABLE USE, MEDIA RELEASE, AND INTERNET

SAFETY PROCEDURES

EMPLOYEE ACCEPTANCE OF TERMS AND CONDITIONS:

These terms and conditions reflect the entire agreement of the parties and supersede all prior oral and written agreements and understandings of the parties.

I have read this contract and understand that should I fail to honor all the terms of this contract it may result in disciplinary action up to and including loss of network privileges, confiscation of computer equipment, termination of employment and/or criminal prosecution.

Employee Name (Please Print)

Employee Signature

Date

I agree to the following release of information:

The school or school district may feature me in the local broadcast and print media, on the school or school district web site, and in district publications and programs.

Employee Name (Please Print)

Employee Signature

Date