Georgia Department of Education

Policies and Procedures

Policy Title:	***Acceptable Use Guidelines for Technology Resources, State Schools***		
Policy Number:	***SS-4003 Descriptor Code-IFBGA***		
Release Date:	***03-02-01***	Last Revised:	***12-17-03***

Purpose

To describe Georgia Department of Education's policy in regard to the acceptable use of technology resources at State Schools.

Applicability

This policy applies to all employees at the three State Schools.

Definitions

Technology Resources: The State Schools' computer systems and networks are any configuration of hardware and software. The systems and networks include all of the computer hardware, operating system software, application software, stored text, and data files. This includes electronic mail, local databases, externally accessed databases (such as the internet), CD-ROM, optical media, clip art, digital images, digitized information, communication technologies, and new technologies as they become available.

Policy

The Department of Education (DOE), the Office of State Schools, and the State Schools reserve the right to monitor all technology resource activity.

General Provisions

The Georgia Department of Education and the Office of State Schools provides technology resources to its students and staff for educational and administrative purposes. The goal in providing these resources is to promote educational excellence in the State Schools by facilitating resource sharing, innovation, and communication with the support and supervision of parents, teachers, and support staff. The use of these technology resources is a privilege, not a right.

With access to computers and people all over the world comes the potential availability of material that may not be considered to be of educational value in the context of the school setting. DOE and the Office of State Schools believes that the value of information, interaction, and research capabilities available outweighs the possibility that users may obtain

material that is not consistent with the educational goals of the State Schools.

Proper behavior, as it relates to the use of computers, is no different than proper behavior in all other aspects of State Schools' activities. All users are expected to use the computers and computer networks in a responsible, ethical, and polite manner. This document is intended to clarify those expectations as they apply to computer and network usage and is consistent with set policy.

Acceptable Use

Technology resources will be used only for learning, teaching, and administrative purposes consistent with established missions and goals. Commercial use of systems is strictly prohibited.

Training will be made available to all users in the proper use of the system and will make copies of the acceptable use guidelines available to all users. All training in the use of the system will emphasize the ethical use of this resource.

Software or external data may not be placed on any computer, whether stand-alone or networked to the system, without permission.

Other issues applicable to acceptable use are:

1. Copyright: All users are expected to follow existing copyright laws.
2. Supervision and permission: Student use of the computers and computer network is only allowed when supervised or granted permission by a staff member.
3. Attempting to log on or logging on to a computer or email system by using another's password is prohibited: Assisting others in violating this rule by sharing information or passwords is unacceptable.
4. Improper use of any computer or the network is prohibited. This includes the following:
    a. Using racist, profane, or obscene language or materials.
    b. Using the network for financial gain, and political or commercial activity.
    c. Attempting to or harming equipment, materials, or data.
    d. Attempting to or sending anonymous messages of any kind.
    e. Using the network to access inappropriate material.
    f. Knowingly placing a computer virus on a computer or the network.
    g. Using the network to provide addresses or other personal information that others may use inappropriately.
    h. Accessing of information resources, files, and documents of another user without their permission

Filtering

The Children's Internet Protection Act requires filtering for minors (1) visual depictions of obscenity, (2) visual depictions of child pornography, and (3) materials harmful to minors. The State Schools will be using SonicPro Firewall Educational Edition software to implement filtering. The filter may be disabled under the following condition.

1. Only authorized personnel may disable the filter for an adult (17 years old and above) to allow research or other lawful use.

System Access

Access to the network systems will be governed as follows:

1. Students will have access to resources for class assignments and research with their teacher's permission and/or supervision.
2. Teachers with accounts will be required to maintain password confidentiality.
3. Employees will be granted access to the system with the approval of the immediate supervisor.
4. System users identified as security risks or as having violated the Acceptable Use Guidelines maybe denied access to the system. Other consequences may also be assigned.

Campus Level Coordinator Responsibilities

As the campus level coordinator for the network systems, the designee will:

1. Be responsible for disseminating and enforcing the Acceptable Use Guidelines for the system at the campus level.
2. Ensure that employees supervising students using the systems provide information emphasizing the appropriate and ethical use of this resource.

Individual User Responsibilities

The following standards will apply to all users of the computer network systems:

1. The individual in whose name a system account is issued will be responsible at all times for its proper use.
2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by guidelines.
3. System users may not use another person's system account without written permission from the campus coordinator or designee, as appropriate.
4. System users are asked to purge electronic mail or outdated files on a regular basis.
5. System users are responsible for making sure they do not violate any copyright laws.

Vandalism Prohibited

Any malicious attempt to harm or destroy equipment or materials, data of another user of the system, or any of the agencies or other networks to which the system has access is prohibited. Deliberate attempts to degrade or disrupt system performance may be viewed as violations of guidelines and, possibly, as criminal activity under applicable state and federal laws. This includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above will result in the cancellation of system use privileges, possible prosecution, and will require restitution for costs associated with system restoration, hardware, or software.

Forgery Prohibited

Forgery or attempted forgery of electronic messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users or deliberate interference with the ability of other system users to send/receive electronic mail is prohibited.

Information Content/Third Party Supplied Information

System users and parents of students with access to the system should be aware that use of the system may provide access to other electronic communication systems outside the network that may contain inaccurate and/or objectionable material.

A student bringing prohibited materials into the school's electronic environment will be subject to a suspension and/or a revocation of privileges on the system and will be subject to disciplinary action. An employee who knowingly brings prohibited materials into the school's electronic environment will be subject to disciplinary action.

Network Etiquette

System users are expected to observe the following network etiquette (also known as netiquette):

1. Using appropriate language: swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language is prohibited.
2. Pretending to be someone else when sending/receiving messages is prohibited.
3. Transmitting obscene messages or pictures is prohibited.
4. Revealing personal information such as addresses or phone numbers is prohibited.
5. Using the network in such a way as to disrupt the use of the network by other users is prohibited.

Termination/Revocation of System User Account

A system user's access to the system may be revoked or suspended upon violation of policy and/or administrative regulations regarding acceptable use.

Termination of an employee's account or of a student's access will be effective on the date the campus coordinator or designee receives notice of user withdrawal or of revocation of system privileges, or on a future date as specified in the notice.

Consequences of Improper Use

Improper or unethical use may result in disciplinary actions consistent with existing policy, or other state and federal laws. This may also require restitution for costs associated with system restoration, hardware, or software.

Disclaimer

The system is provided on an "as is, as available" basis. The DOE, the Office of State Schools, and the State Schools do not make any warranties, whether expressed or implied, including, without limitation, those of fitness for a particular purpose with respect to any services provided by the system and any information of software contained therein. A variety of vendor supplied hardware and software is used. Therefore, the Department of Education and the Office of State Schools does not warrant that the functions or services performed by, or that the information of, software contained on the system will meet the user's requirements. Neither does it warrant that the system will be uninterrupted or error-free, nor that defects will be corrected. Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third party individuals in the system are those of the providers and not necessarily the State Schools, DOE, and the Office of State Schools. State Schools, DOE, and the Office of State Schools will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the computer systems and networks.

Electronic Mail and Additional Technology Guidelines

1. Electronic Mail (e-mail) via Network Application
2. User Security Responsibilities
3. Maintenance of Local Hard Drives
4. Software and Hardware Procurement

Electronic Mail

E-mail has become one of the most used communication tools in both offices and classrooms. As it becomes a part of all classrooms as well as most office areas, the following points are important to keep in mind:

1. LotusNotes is the only e-mail system to be used by employees at the State Schools.

2. The software and hardware that provides us e-mail capabilities for the State Schools has been publicly funded. For that reason, it should not be considered a private, personal form of communication. Although staff does not actively monitor communications, the contents of any communication of this type would be governed by the Open Records Act. State Schools abide and cooperate with any legal request for access to e-mail contents by the proper authorities.

3. Any data that is confidential and sensitive in regard to student or staff information shall not be transmitted to or from e-mail accounts such as Yahoo, AOL, BellSouth, Hotmail, Comcast, or any other e-mail account/system outside of LotusNotes. This includes but is not limited to information that is covered under the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPPA). Confidential or sensitive information shall only be transmitted from a LotusNotes account to a LotusNotes account. Using the encryption feature of LotusNotes is highly suggested when transmitting confidential and sensitive data. Any sensitive information should be delivered via a compact disc which is password protected or through other similar safe means of delivery.

4. Since e-mail access is provided as a normal operating tool for an employee's job performance, individual staff e-mail addresses must be shared with interested parents and community members who request to communicate with staff in this fashion. Each campus and department should post a list of e-mail addresses for their staff through their Internet pages.

5. Staff should be expected to return e-mail communications to parents or other public members having a legitimate business request within 24 hours whenever possible. Requests from outside agencies for information do not fit into this same category and can be handled with a different timeline or in a manner consistent with previous experience in working with similar requests. Staff should not participate in e-mail surveys without authorization.

6. Incoming e-mail that is misaddressed will remain "undeliverable." Staff is not available to personally inspect all messages of this type and forward them to the proper person. Please be certain to give your correct e-mail address. All Internet pages containing lists of staff addresses should also contain a disclaimer that makes everyone aware that e-mail not responded to in a 24-hour timeframe should be resent.

7. During student contact time in the classroom, your e-mail notifier should be turned off to prevent interruptions. Staff members should set aside time at least once a day to check and respond to e-mail messages.

E-mail does not have to be answered immediately; simply allow enough time so that the 24-hour turnaround time can be met in most instances.

8. Since e-mail access is provided for school business related use, please do not forward messages that have no educational or professional value. An example would be any number of messages that show a cute text pattern or follow a "chain letter" concept. These messages should be deleted and the sender notified that messages of that nature are not appropriate to receive on your school e-mail account.

9. Please use the "groups" function of our e-mail system appropriately. Do not send messages to an entire staff when only a small group of people actually needs to receive the message.

10. Attachments to e-mail messages should include data only files. At no time should program files (typically labeled ".exe") be attached due to software licensing requirements. In addition, there exists the real possibility that any program files received as attachments over the Internet may include viruses or other very destructive capabilities once they're "launched" or started. If you receive an attachment like this, please delete the e-mail message immediately without saving or looking at the attachment.

11. Subscriptions to Internet listservs should be limited to professional digests due to the amount of e-mail traffic generated by general subscription. Please use your personal Internet account to receive listserv subscriptions of a general nature, if available.

12. Students will not be issued individual e-mail accounts. For any projects that involve e-mail communications, use either your district account as facilitator to the activity, or work with your technology coordinator to activate a special project account for a limited time.

13. Please notify your technology coordinator if you receive unsolicited e-mail, particularly if it is of a "hate mail" nature. An attempt will be made to track down the source of that e-mail and prevent any additional unsolicited mail.

User Security Responsibilities

1. Your username and password should be protected from unauthorized use at all times. Do not post this information where others can view it.
2. Do not share your password via e-mail at any time. If a technology representative needs that information, they must request it in person.
3. You should use your screen saver to secure your computer whenever it is not in use, and it should be password protected.

Maintenance of Local Hard Drives

1. On occasion, hard drives must be reformatted. Reformatting completely erases all contents of the hard drive. We will not reinstall unapproved copies of software nor will we be able to retrieve any personal data files. Only approved copies of software will be reinstalled. Be personally responsible for making backups of any data files that are stored on your local hard drive.
2. All computer and video hardware should be shut down each evening unless instructed by the technology coordinator to do otherwise. This includes CPUs, monitors, and VCRs. The exception to this would be laser printers. They can be left on since they include automatic power-saving features.

Software and Hardware Purchases

1. The identified process for purchasing software should be followed. No software packages can be purchased at the campus or department level without following that process.
2. It is important to keep in mind that no software should, or will, be installed without documentation that shows the software purchase has gone through the purchasing process and that proper licensing has been purchased.
3. Similarly, all hardware purchases should be those items that are designated as meeting state standards for procurement.

Authority and/or Cross-Reference

- DOE *Internet and E-mail Usage* Policy (HR-1108)
- Family Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPPA)