



School/Location Computer Security
Incident Reporting Procedures
External

Version 2.0

Version	Date	Update origin	Written by	Verified by
2.0	August 19, 2009	Original	Graves, Mark	Brown, Bill

Greenville County Schools

School/Location Computer Security Incident Reporting Procedures External

1. Introduction	4
1.1. Examples of possible computer security incidents.....	4
2. Incident handling process	4
2.1. Report a possible incident to the ETS Help Desk.	5
2.2. ETS Help Desk takes initial actions.....	5
2.3. Information Security takes over the process.	5
2.4. Information Security will issue a confidential incident report.	5
2.5. Information security closes the incident.	5
3. District Acceptable Use Policy (Board Rule EFE).....	6
4. Definitions and law.....	15
4.1. Definitions	15
4.2. Relevant South Carolina Law.....	15
5. South Carolina Computer Crime Law	16
6. SC 16-3-1040, Offenses against the person	21
7. SC 16-17-430, Offenses against public policy	21

1. Introduction

With the increasing use of computers and networks at Greenville County Schools (GCS), the risk of policy or law violations involving computers is increasing. Most incidents involve students or staff. Personal awareness, particularly in the classroom, is key to identifying policy violations. A student or staff member may be the victim or the perpetrator. In either case, following proper procedures is imperative. Crimes and policy violations are not only committed against computers (hacking), but computers are also used to commit non-computer related violations such as harassment or unethical conduct.

1.1. Examples of possible computer security incidents

- Any violation of the district rule EFE which is the district computer acceptable use policy for staff and students. For the policy see section 3 or <http://www.greenville.k12.sc.us/gcsd/depts/ets/policy/aup.asp>.
- Attempted or actual unauthorized access to any district system including email accounts.
- Student or employee computer activity violating South Carolina, or Federal Law. For SC computer crime law see Section 5.
- Using district computers or networks to attempt unauthorized access to non-district systems.
- Viewing or downloading objectionable material on the district network or using a district computer to do so when at a non-district location.
- Using a computer for unlawful communication such as harassment.
- Attempting to or using another's login to gain unauthorized access to district systems.
- Bypassing or attempting to bypass district web filters or proxy servers.
- The spread of viruses or other malicious software into the GCS network.
- Unauthorized person trying to gain information about GCS information systems through phone calls, in person, or email.
- Suspicious email, beyond common SPAM, particularly trying to gain information about GCS computers or networks.
- Unauthorized person trying to gain physical access to GCS computers or network equipment.
- Physical theft of computer, server, notebook, network equipment, or PDA or any other district information.
- Unauthorized installation of equipment on the district network or repair of district equipment by non-ETS personnel.
- Intentional or accidental information breach.
- Attempt to disable district system controls.

2. Incident handling process

In the event of a suspected computer incident, the procedures outlined below must be followed. Do not delay reporting it to Education Technology Services (ETS) at 355-4357, as lapsed time makes the investigation more difficult.

Initial investigation by Information Security is essential to determine if there is an actual incident and to prevent further harm. After the initial investigation, Information Security will inform the school or location administration of the incident details. The process is as follows:

2.1. Report a possible incident to the ETS Help Desk.

Contact the ETS Help Desk at 355-4357 to report a possible incident. When contacting the Help Desk, be sure to provide information such as users and computers involved or symptoms you notice. Also provide district cell numbers of location administration so Information Security can easily contact them. Key information to report includes:

- Date and time the incident was discovered
- Service tag and IP address of the computer(s) used
- Programs in use
- Screens or error messages on the computer
- User IDs of the person(s) in question

2.2. ETS Help Desk takes initial actions.

The ETS Help Desk may take initial actions such as disabling associated user accounts. This will cause some inconvenience to the affected users. They will also contact Information Security. Information Security will work to reduce inconvenience as much as possible.

2.3. Information Security takes over the process.

Information Security will proceed according to the internal computer security incident response plan. Information Security may collect hard drives and other storage media. Collecting hard drives and storage media will inconvenience affected users. Information Security will attempt to reduce user inconvenience as much as possible. However, resolving the incident is the top priority. All communication regarding the incident is confidential.

2.4. Information Security will issue a confidential incident report.

Information Security will issue a confidential incident report to executive management.

2.5. Information security closes the incident.

Information Security will close the incident when it is resolved and re-enable and disable user accounts according to the resolution of the incident.

3. District Acceptable Use Policy (Board Rule EFE)

I. Introduction

Each employee, contractor, or non-student user of Greenville County Schools (“GCS”) information systems at GCS is expected to be familiar with and consistently follow the baseline control measures that this rule defines. These security measures, sometimes called “standard of due care controls”, are the minimum controls required to prevent problems like fraud and embezzlement, sabotage, errors and omissions, system unavailability, and various legal problems, such as allegations of negligence, breach of fiduciary duty, and privacy violation.

II. Legal Requirements

GCS management is committed to complying with applicable information security legislation and relevant information security standards and requirements. These include, but are not limited to the following:

- The Family Educational Rights and Privacy Act (FERPA)
- Children’s Internet Protection Act (CIPA)
- Protecting Children in the 21st Century Act
- Health Insurance Portability and Accountability Act (HIPAA)
- Individuals with Disabilities Education Act (IDEA)

Users of the network are responsible for respecting and adhering to local, state, federal, and international laws. Any attempt to break those laws through the use of GCS information systems may result in litigation against the offender by the proper authorities. If such an event should occur, GCS will fully cooperate with the appropriate authorities to provide any information necessary for the civil and/or criminal litigation process.

III. Employee Technology Acceptable Use Rule

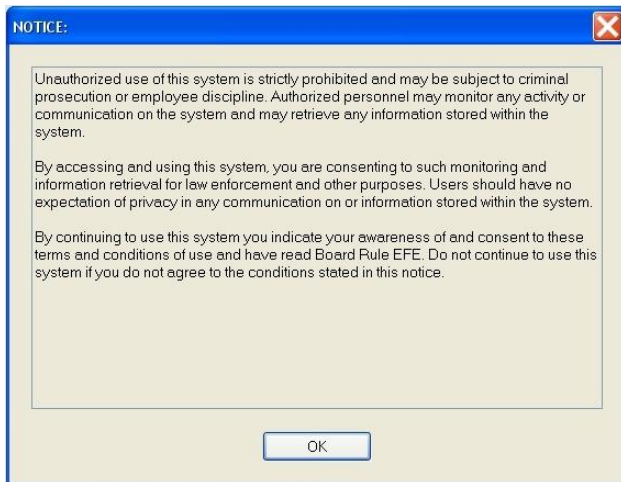
The purpose of this directive is to provide GCS employees with guidance on the proper use of the district’s information technology resources, including but not limited to:

- The Internet, the Intranet, e-mail, and Portal
- District assigned computing devices such as cell phones, PDAs, portable computers, and portable storage,
- The district’s network and supporting systems and the data transmitted by and stored on these systems.

The use of the district technology resources is a privilege granted to employees for the enhancement of job-related functions. Employees may have limited access to these resources for personal use, if they comply with the provisions of this rule. Violations of this rule may result in the revocation of this privilege. Employees may also face disciplinary action up to and including termination, civil litigation, and/or criminal prosecution for misuse of these resources.

A. Annual Responsibilities and Information Security Awareness:

Each year every staff member must review the Information Security Awareness materials on the GCS Portal web site. Every GCS computer resource presents a notification prior to logon that reviewing this rule is mandatory.



B. Prohibited Uses of GCS Computer Resources:

- Unauthorized or excessive personal use.
- Use of GCS computer resources to infringe the intellectual property rights of others.
- Use of GCS computer resources for personal profit.
- Use of GCS computer resources to further political causes.
- Staff shall not upload or otherwise transfer out of the district's direct control any software licensed to the district or data owned or licensed to the district without explicit written authorization. Failure to observe copyright or license agreements may result in disciplinary action from GCS or legal action by the copyright owner.
- Staff shall not use IT resources (including but not limited to servers, networks, workstations, and printed output) to reveal confidential or sensitive information, student data, or any other information covered by existing state or federal privacy or confidentiality laws, regulations, rules, policies, procedures, or contract terms. Staff who engages in the unauthorized or accidental release of confidential information via the district's IT resources will be subject to sanctions in existing policies and procedures associated with release of such information.
- Staff shall not download executable software, including freeware and shareware, unless it is required to complete their job responsibilities.
- Staff shall not bypass or attempt to bypass any of the District's security or content filtering safeguards. See section V. B. for more information.
- Staff shall not use district IT resources to intentionally disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of the district's IT resources.
- Staff shall not access, store, display, distribute, edit, or record sexually explicit or extremist material using district IT resources.
- Violation of this rule may result in immediate disciplinary action. The incidental and unsolicited receipt of sexually explicit or extremist material, such as might be received through e-mail, shall not constitute a violation of this section, provided that the material is promptly deleted and neither stored nor forwarded to other parties.
- Staff is prohibited from accessing or attempting to access IT resources for which they do not have explicit authorization by means of user accounts, valid passwords, file permissions or other legitimate access and authentication methods. It is a violation of district rule to grant another individual access to any district accounts that have been authorized to you; or use another individual's district authorized accounts, user-ids and/or passwords. Specific exceptions are allowed for ETS personnel for authorized system operations and maintenance.
- Staff shall not allow another person to use a district system under his or her district login or student login.
- Staff shall not add, modify, repair, remove, reconfigure or otherwise tamper with any device on the network infrastructure including, but not limited to: wireless network devices, workstations, printers, servers, cabling, switches/hubs, routers, etc. Changes to GCS information systems must be performed by authorized personnel under the auspices of ETS.

- "Hacking tools" which may be used for "computer hacking" as defined in the South Carolina Computer Crime Act, may not be possessed on any district premise or run or loaded on any district system except for authorized use by ETS.

- District equipment taken off-site may only be used by district employees. Under no circumstances are non-district persons permitted to use district assigned information systems without written permission from ETS. The “Employee Technology Acceptable Use Rule” applies to the use of district computing resources even when off-site.

C. User Passwords

Staff members receive a unique user ID for GCS network and computer use. The accompanying password is not to be shared. Staff may change their password at any time and may be required to change it at regular intervals according to GCS security standards.

D. Access to Information System Rooms

Staff members may only grant access to sensitive areas such as server rooms, wiring closets, etc, after they have verified with the ETS Help Desk the credentials and need for access of the person requesting access. Hard copy logs of information system room access must be maintained.

E. Sensitive Information

Staff members may not disclose sensitive information to persons not authorized to receive it. This includes non-public information such as Social Security Numbers, credit card numbers, bank account numbers, health information, or confidential student data. Sensitive hardcopy information must be securely stored according to GCS policies and be destroyed by shredding when no longer needed.

All employees who have access to or may have access to personally identifiable student records shall adhere to all standards included in the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), and other applicable laws and regulations, as they relate to the release of student information.

F. Limited Personal Use

Occasional and incidental personal use of the district’s IT resources and Internet access is allowed subject to limitations. By the allowance of such use, however, the GCS does not grant any ownership, privacy, or expectation of privacy to any person in the contents of any messages or other Internet activities involving GCS resources or equipment.

Personal use of the Internet is prohibited if:

- It materially interferes with the use of IT resources by the district; or
- Such use burdens the district with additional costs; or
- Such use interferes with the staff member’s employment duties or other obligations to the district; or
- Such personal use includes any activity that is prohibited under any district (including this rule), state or federal statute or policy.

G. E-Mail

Inappropriate E-Mail Messages Each district e-mail user is responsible for the content of all text, audio or images that they place or send over the Internet or district email systems. Fraudulent, harassing or obscene messages are prohibited. All messages communicated on the Internet should have the sender’s name attached. No messages will be transmitted under an assumed name. You may not use another’s e-mail address to send e-mail messages. Users may not attempt to obscure the origin of any message.

Information published on the Internet should not violate or infringe upon the rights of others. No abusive, profane or offensive language may be transmitted through the system.

Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual or group’s race, religion, gender, age, national origin, physical attributes, disabilities, or sexual preference will be transmitted.

E-Mail Addresses: Employees must only use official district e-mail address for all district business matters. The use of anonymous e-mail services such as yahoo, gmail, msn, etc on the GCS network is prohibited.

Forwarding E-Mail Externally: Employees must not forward confidential or sensitive district emails to a non-district email address that they own or control.

Retention of E-Mail Messages: An e-mail message must be retained for future reference if it contains information relevant to the completion of a district transaction, contains potentially important reference information, or has value as evidence of a district or school management decision. The e-mail message should be printed and filed accordingly.

E-Mail Message Storage Schedule and Allotment: E-mail will be backed up for only fourteen calendar days, and each employee will be limited to a total of 200MB of message storage space. Employees must delete messages they don't need, and store messages that they will need in another way besides the electronic mail system. Examples of this are printing, saving to other document types, and archiving messages in off-line email folders.

Public Information: E-mail messages are considered public records and are therefore legally discoverable.

H. IT Resource Monitoring

GCS may install software and/or hardware to monitor and record all IT resources, usage, including e-mail and Web site visits. The district retains the right to record or inspect any and all files stored on or transmitted by district systems.

Staff shall have no expectations of privacy with respect to district IT resource usage. Staff is advised that serious disciplinary action may result from evidence of prohibited activity obtained through monitoring or inspection of electronic messages, files, or electronic storage devices. Illegal activity involving district IT resource usage may be referred to appropriate authorities for prosecution.

I. Consequences

Violators of the GCS Employee Technology Acceptable Use Policy may be subject to disciplinary action, charge backs for time and materials to repair GCS damaged IT Resources or otherwise harmed through the addition, removal, reconfiguration, or any other changes not specifically authorized by ETS.

IV. Student Acceptable Use Policy Agreement

The School District of Greenville County provides computer, network, e-mail, and Internet access to students as part of the learning environment. While these systems have the power to deliver a huge number of resources to our classrooms, their ability to serve students depends on the responsible and ethical use of them by every student.

GCS may install software and/or hardware to monitor and record all information system resources, usage, including e-mail and Web site visits. The district retains the right to record or inspect any and all files stored on district systems.

Students shall have no expectation of privacy with respect to district information system resource usage. Students are advised that serious disciplinary action may result from evidence of prohibited activity obtained through monitoring or inspection of electronic messages, files, or electronic storage devices. Illegal activity involving district information system resource usage may be referred to appropriate authorities for prosecution.

“Acceptable use” of these systems is use that is consistent with the instructional goals of the District. If you break “acceptable use” rules, you may lose the privilege to use both classroom computers and/or the Internet. Further disciplinary and/or legal action may be taken at the discretion of school administration.

The District takes reasonable precautions by using filtering software to keep inappropriate Internet sites and e-mail out of the classroom. The District does not supervise individual e-mail accounts, a Parent Portal is available that permits the supervision of your child's e-mail account.

Please note that parents may choose for their child not to have access to the Internet at school; however, students who do not have access to the Internet will not be able to access e-mail or web based programs that teachers may be

using in class. Your child has agreed to the terms and conditions of this document upon acceptance of the school district handbook. Violation of any of the terms or conditions will result in disciplinary action and/or involvement of law enforcement.

Treat computer equipment with care and respect – Willful destruction of any computer equipment or software will be considered vandalism, and may warrant the involvement of local law officials.

Parents and guardians, by you and your child agreeing to this acceptable use policy you will insure that GCS computer equipment is handled with care and respect. Only GCS ETS personnel are allowed to repair or modify GCS computer equipment hardware and software.

Do not add, modify, repair, remove, reconfigure or otherwise tamper with any device on the network infrastructure including, but not limited to: wireless network devices, workstations, printers, servers, cabling, switches/hubs, routers, etc

Do not perform unauthorized access, use, or attempt unauthorized access or use of District information systems.

“Hacking tools” Hacking tools” which may be used for “computer hacking” as defined in the South Carolina Computer Crime Act, may not be possessed on any district premise or run or loaded on any district system. Do not use school computers for illegal activities such as planting viruses, hacking, or attempted unauthorized access to any system. This is an automatic recommendation for expulsion.

Do not use a cell phone or PDA to access the Internet on school premises.

Any written text, graphics or executable files created, downloaded, displayed, or exchanged with another student or teacher must be for education-related purposes only.

Do not bypass or attempt to bypass any of the District’s security or content filtering safeguards.

Do not use school computers for commercial purposes.

Follow copyright laws at all times – See District copyright policies for more information. If you have questions about the legality of using software, text, graphics, or music you find online, ask your teacher or media specialist for guidance.

Keep your password secret – You will be held responsible for all computer activities associated with your password. For example, if you share your password with your friend and he/she signs on as you and breaks one of the rules outlined above, you will be held responsible.

Do not allow another person to use the computer under your district login.

All online communication must be polite and not threatening or offensive in any way – All students in grades 3-12 are issued e-mail accounts. The District has the right to review any e-mail sent or received using District equipment and e-mail accounts. E-mail accounts should be used for educational and district purposes only.

Do not give out personal information or photos through online communications (i.e. e-mail, cell phone, PDA, etc). Never give out your phone number, social security number, full name, age, home address, or any other personal information.

Home directories are provided to students for educational related work. Students should not store personal or non-school related work in home directories. The District reserves the right to review the contents of a student’s home directory.

Please contact your school if you do not want your child to have access to the Internet and e-mail.

V. GCS “ Internet Safety Policy” (Staff and Students)

This rule includes provisions to address access by minors to inappropriate matter on the Internet and World Wide Web; the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communication; unauthorized access, including so-called “hacking” and other unlawful activities by minors online; unauthorized disclosure, use, and dissemination of personal identifications regarding minors; and measures designed to restrict minors’ access to materials harmful to minors.

A. General Access. The smooth operation of the network, Internet, and e-mail services relies on the proper conduct of the end users who must adhere to strict guidelines. These guidelines are provided so that students and staff are aware of their responsibilities when using these technologies. In general, this requires efficient, ethical, and legal utilization of the network resources. Because access to the network provides connections to other computer systems located all over the world, users (and parents of students who are users) must understand that neither the District nor any District employee controls the content of the information available on the systems. Every effort will be made by the District to monitor and restrict ready access to known objectionable sites; however, the District does not condone the use of controversial or offensive materials and cannot be held responsible for such use.

B. Technology Protection Measures. In compliance with the Children’s Internet Protection Act (“CIPA”), 47 U.S.C. § 254 (h), the District uses technological devices designed to filter and block the use of any of the District’s computers with Internet access to retrieve or transmit any visual depictions that are obscene, child pornography, or “harmful to minors” as defined in the CIPA. Though the district makes reasonable efforts to filter such Internet content, the district cannot warrant the effectiveness of its Internet filtering due to the dynamic nature of the Internet

Adult users of a District computer with Internet access may request that the “technology protection measures” be temporarily disabled by the chief building administrator of the building in which the computer is located for bona fide research purposes or other lawful purposes not otherwise inconsistent with this administrative rule.

C. Education, Supervision, and Monitoring. It shall be the responsibility of all district school staff to educate, supervise, and monitor appropriate usage of online computer network and access to the Internet in accordance with this policy, CIPA, and the Protecting Children in the 21st Century Act.

D. Terms and Conditions of Use

1. Acceptable Use. The purpose of the District’s educational network is to support research and education by providing access to unique resources and the opportunity for collaborative work. All use of the network, Internet, and e-mail services must be in support of education and research and consistent with the educational objectives of the District. Use of other networks or computing resources must comply with the guidelines governing those networks. Transmission of any material in violation of any federal or state laws or regulations is prohibited; this includes, but is not limited to, copyrighted material, threatening or obscene material, or material protected by trade secret. Access to computer systems, personally assigned district computing devices, and networks owned or operated by the District imposes certain responsibilities and obligations on users and is subject to District policies and local, state, and federal laws. Acceptable use is always ethical, reflects honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of information, system security mechanisms, and the individual’s rights to privacy and freedom from intimidation, harassment, and unwarranted annoyance.

2. Procedures for Use

1. Administrators and teachers may access the Internet or e-mail for educational or work-related purposes at any time, which is not disruptive and does not interfere with the performance of other responsibilities by the employee.
2. The District will notify parents/guardians about the District network, related safety issues, and issues governing its Internet through a general letter to all parents. Parental permission is not required for use of the Internet, but parents will be notified they have the right to file a Parent/Guardian Denial Form available from the school principal if they do not want their child(ren) to have access to Internet resources.
3. A student’s parent or guardian must sign a Student E-mail Account Agreement in order for that student to be granted an individual e-mail account. The parent/guardian may withdraw approval at any time through a written request directed to the student’s teacher or principal.

4. All computer, Internet usage and e-mail usage by District employees and students must be consistent with the Greenville County School District mission and policies.

3. Rules Governing Use

Permitted Uses of Internet and E-mail

- **Users** will utilize the system for educational and professional or career development activities only, except as permitted in Article III (F).
- **Users** may download text and other non-executable files attached to e-mail messages or from the Internet for school-related business only.
- **Users** will check their e-mail frequently, delete unwanted messages promptly, and stay within their e-mail quota. Be aware that the system administrator may delete e-mail at any time.

General Prohibitions

- **Users** may not use the District system for commercial purposes, defined as offering or providing goods or services or purchasing goods or services for personal use. Greenville County School District will not be responsible for any obligations resulting from any unauthorized use of the system.
- **Users** may not use the system for political activities.
- **Users** will not post chain letters or engage in spamming. Spamming is sending an unnecessary message to a large number of people.

Personal Safety

- **Students** will not post or e-mail personal contact information about themselves or other people unless it is in conjunction with a specific teacher-approved assignment or approved college/career communication. Personal contact information includes address, telephone number, school address, etc.
- **Students** will not agree to meet with someone they have met online without their parent/guardian's approval.
- **Students** will promptly disclose to an administrator, teacher, or other school employee any message they receive that is inappropriate or makes them feel uncomfortable.

Illegal Activities

- **Users** will not attempt to gain unauthorized access to the e-mail system, the District Web pages, or any other computer systems through Greenville County School District e-mail and/or Internet and/or network access. Users will not attempt to perform functions that exceed their authorized access. This includes attempting to log in through another person's account or access another person's files. These actions are illegal.
- **Users** will not make deliberate attempts to disrupt the computer system performance or destroy data by spreading computer viruses or by any other means. These actions are illegal.
- **Users** will not use the District system to engage in any other illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of another person, or any other activity that violates existing District policies or procedures. Reference to such activities will not even be made in a joking manner or as a prank.
- **The District** will notify law enforcement should illegal activities take place.

System Security

- **Users** will not share their account information (User ID and/or password) or attempt to log in to another user's account. Any sharing of User ID or password will result in immediate restriction or removal of account privileges. The only potential exception is the sharing of information with IT staff if requested for troubleshooting purposes.
- **Users** will immediately notify the IT staff if they have identified a possible security problem (students should notify a teacher and/or principal). Do not actively seek security problems but immediately report any potential issues that are found.
- **Users** will not download or install any unauthorized software or install any unauthorized hardware.
- **Users** will not run any executable files attached to an e-mail message.
- **Users** will not knowingly use portable data storage devices, which contain viruses or in any other way knowingly spread computer viruses.

Use of Appropriate Language

Restrictions against inappropriate language may apply to public messages, private messages, and material posted on Web pages.

- **Users** will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or gang related language or symbols.
- **Users** will not post or e-mail information, which could cause damage or a danger of disruption.
- **Users** will not engage in personal attacks, including prejudicial or discriminatory remarks.
- **Users** will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending messages, he/she must stop.
- **Users** will not use any language in an e-mail that threatens another person, whether it is the recipient of the message or a third party.
- **Users** will not knowingly or recklessly post false or defamatory information about a person or organization.

Access to Inappropriate Material

- **Users** will not use the District system to access or send material that is profane, lewd, vulgar, indecent, libelous, or obscene, e.g., pornography, that advocates illegal acts, or that advocates violence or discrimination towards other people, e.g., hate literature.
- **Adult Users** who mistakenly access inappropriate information or images should immediately report this to ETS. This will initiate proceedings to have the materials blocked.
- **Students** who mistakenly access inappropriate information or images should immediately report this to the attending teacher. ETS should be notified if it is deemed warranted. This will protect the users against an allegation that they have intentionally violated the Acceptable Use Policy.
- **Students** are expected to follow parental guidance regarding limitation of access to additional types of inappropriate materials.

Respect for Privacy

- **Users** will not repost or e-mail a message that was sent to them privately without permission from the person who originally sent the message.
- **Users** will not post or e-mail private information about another person.

E. Penalties for Improper Use. An employee who violates the terms of this administrative rule or otherwise misuses e-mail or the Internet to access or send inappropriate material will be subject to disciplinary action, up to and including discharge. In addition, the privilege of accessing the Internet and e-mail services also will be subject to cancellation. Students who violate the terms of this administrative rule or who otherwise misuses their access to e-mail or the Internet also will be subject to disciplinary action in accordance with the District Student Behavior Code. Internet and e-mail access privileges also may be cancelled. Violations of the laws of the United States or the State of South Carolina also may subject student or employee users to criminal prosecution. If a user incurs unauthorized costs, the user, as well as the user's parents if the user is a student, will be responsible for all such costs.

F. Warranty. The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages suffered by any user. This includes loss of data resulting from delays, non-deliveries, misdirected deliveries, or service interruptions caused by the system's negligence, user errors, or omissions. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

G. Security. Security on any computer system is a high priority, especially when the system involves many users. If a student or employee believes he/she has identified a security problem on the network, he/she must notify the administrator for the school or ETS. Do not demonstrate the problem to other users. Attempts to log on to any network as a system administrator will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be subject to severe restrictions, cancellation of privileges, or other disciplinary and/or legal action.

H. User Privacy. E-mail messages sent or received via a District-issued e-mail account and all other electronic files created using District resources or stored with District resources are property of the District. The District reserves the right to examine, restrict, or remove any material that is on or passes through its network, just as it does any other work or material generated or brought to school by staff or students. Access to electronic information related to any student or staff member will be governed by the same policies that would apply to that information if it were not in electronic form.

I. School Board Policies. All documents on the District’s server(s) must conform to Board policies and regulations, as well as established school guidelines. Copies of Board policies are available on Board Docs. Persons developing or maintaining Web documents are responsible for complying with these and other policies. Some of the relevant issues and related Board policies include the following:

1. Electronic transmission of materials is a form of copying. As specified in District policy, no unlawful copies of copyrighted materials may be knowingly produced or transmitted via the District’s equipment, including its Web server(s).
2. Documents created for the Web and linked to District Web pages must meet criteria for use as an instructional resource.
3. Any links to District Web pages that are not specifically curriculum-related must meet the criteria established in the District Internet Authorized Use policy. Any other non-curricular materials should be limited to information about other youth activities, agencies, or organizations which are known to be non-sectarian, exclusively devoted to community interests or child welfare, non-profit, and non-discriminatory. Web page links may not include entities whose primary purpose is commercial or political advertising.
4. All communications via District Web pages will comply with the District Acceptable Use for Network, Internet, and E-mail Services Policy and the District Student Behavior Code. Offensive behavior that is expressly prohibited by this policy includes religious, racial, and sexual harassment and/or violence.
5. Any student information communicated via District Web pages must comply with District policies on Data Privacy and Public Use of School Records.
6. Links to external websites (e.g. blogs, forums, social networking sites, non-instructional sites) from a district/school/teacher website or from a district e-mail signature are prohibited.
7. Blogs or forums used for instruction must reside on district web servers.
8. Personal blogs and social networking sites must not link to any district web site or district e-mail address.

J. OTHER

1. Material on a Web page reflects an individual’s thoughts, interests, and activities. Such Web pages do not, in any way, represent individual schools or the District, nor are they endorsed or sanctioned by any individual school or the District. Concern about the content of any page(s) created by students or staff should be directed to the building principal of that school or to that school’s media specialist.
2. Given the rapid change in technology, some of the technical standards outlined in this rule may require change throughout the year. Such changes will be made with approval of the Superintendent. This rule may be updated on an annual basis or more frequently if required.

VI. Access Control Rule

Public information is available at the GCS web site, and Internal Use Only information is available on the GCS internal web sites without a login. Access to Confidential or other sensitive information is granted only when a legitimate business need has been demonstrated and access has been approved in advance by the information Owner. Access to special hardware and software must be restricted based on business need. Education Technology Services (“ETS”) will develop and maintain specific written procedures regarding access control.

VII. Systems Application and Development Rule

ETS will develop and maintain specific written procedures for systems application and development. All systems and applications development and/or changes must adhere to GCS security policies, rules, and standards.

VIII. Education Technology Systems Operations Rule

ETS shall develop and maintain specific written procedures for systems operations, including system security.

IX. Information System Procurement Rule

A formal risk assessment shall be performed for all GCS information system procurement and grants. This risk assessment shall be used by ETS to determine the controls needed to mitigate risk to acceptable levels or to deny the purchase or grant.

4. Definitions and law.

4.1. Definitions

Computer: A detailed definition is found in Section 4, South Carolina Computer Crime Law. "Computer" includes, but is not limited to, mainframes, servers, workstations, desktops, and notebooks. It also includes portable hand-held computing devices such as personal digital assistants and digital cellular telephones; data communications network devices such as routers and switches.

Hacking: Accessing or attempting to access all or part of a computer, computer system, or a computer network without express or implied authorization for the purpose of establishing contact only. It also involves using a group of computer programs commonly known as "port scanners" or "probes" to intentionally access any computer, computer system, or computer network without permission. For more detail see Section 4, South Carolina Computer Crime Law

Objectionable material: Downloading to a GCS computer, accessing from a GCS computer, or viewing information on GCS computers which violates employee policy and student codes of conduct. The federal Children's Internet Protection Act also addresses this:
<http://www.fcc.gov/cgb/consumerfacts/cipa.html>.

Malicious software: Unauthorized software that is intentionally installed on a computer to cause harm, disrupt computer operations, or to provide unauthorized access. This includes viruses, trojans, worms, and bots. For descriptions see http://www.cisco.com/web/about/security/intelligence/05_09_Virus-Worm-Diffs.html.

Web filter: A computer through which all student Internet web connections must pass to deny access to objectionable sites.

Proxy server: A computer through which all student Internet web connections must pass to force it through the web filter.

4.2. Relevant South Carolina Law

4.2.1. Computer Crime Law, SC 16-16-10.

Generally deals with what is known as hacking. See Section 5 for the text or see <http://www.scstatehouse.net/code/t16c016.htm>

4.2.2. Offense against persons, SC 16-3-1040

This defines "threatening life, person or family of public official or public employee." Teachers are included as public employees. See Section 6 for the text or see:

<http://www.scstatehouse.net/code/t16c003.htm>

4.2.3. Unlawful communication SC 16-17-430

This defines unlawful electronic communication which includes "words or language of a profane, vulgar, lewd, lascivious, or an indecent nature." See Section 7 for the text or

<http://www.scstatehouse.net/code/t16c017.htm>

5. South Carolina Computer Crime Law

<http://www.scstatehouse.net/code/t16c016.htm>

**South Carolina Code of Laws
(Unannotated)
Current through the end of the 2005 Regular Session
Disclaimer**

This statutory database is current through the 2005 Regular Session of the South Carolina General Assembly. Changes to the statutes enacted by the 2006 General Assembly, which will convene in January 2006, will be incorporated as soon as possible. Some changes enacted by the 2006 General Assembly may take immediate effect. The State of South Carolina and the South Carolina Legislative Council make no warranty as to the accuracy of the data, or changes which may have been enacted since the 2005 Regular Session or which took effect after this database was prepared and users rely on the data entirely at their own risk.

**Title 16 - Crimes and Offenses
CHAPTER 16.
COMPUTER CRIME ACT**

SECTION 16-16-10. Definitions.

For purposes of this chapter:

- (a) "Computer" means a device that performs logical, arithmetic, and memory functions by manipulating impulses including, but not limited to, all input, output, processing, storage, computer software, and communication facilities that are connected or related to a computer in a computer system or computer network. For the purposes of this section, "computer" includes, but is not limited to, mainframes, servers, workstations, desktops, and notebooks; industrial controls such as programmable logic controllers and supervisory control and data acquisition systems; portable hand-held computing devices such as personal digital assistants and digital cellular telephones; data communications network devices such as routers and switches; and all other devices that are computer-based or communicate with or are under the control of a computer such as appropriate telephone switches, medical devices, and cable and satellite television interface systems. "Computer" does not include automated typewriters or typesetters.
- (b) "Computer network" means the interconnection of two or more computers, and those devices and facilities through which an interconnection occurs.
- (c) "Computer program" means a series of instructions or statements executable on a computer, which direct the computer system in a manner to process data or perform other specified functions.
- (d) "Computer software" means a set of computer programs, data, procedures, or associated documentation concerned with the operation of a computer system.
- (e) "Computer system" means a set of related, whether connected or unconnected, computer equipment, devices, or software.

(f) "Property" includes, but is not limited to, financial instruments, data, documents associated with computer systems, and computer software, or copies thereof, whether tangible or intangible, including both human and computer system readable data, and data while in transit.

(g) "Services" include, but are not limited to, the use of the computer system, computer network, computer programs, or data prepared for computer use, or data obtained within a computer system, or data contained within a computer network.

(h) "Data" means a representation of information, knowledge, facts, concepts, or instructions that has been prepared or is being prepared in a formalized manner and has been processed, is being processed, or is intended to be processed in a computer, computer system, or computer network. Data may be in any form including, but not limited to, computer printouts, magnetic storage media, optical storage media, network data packets, flash memory cards, smart card memory, punched cards, or as stored in the memory of the computer or in transit or displayed on a video device.

(i) "Access" means to gain entry to, attempt to gain entry to, instruct, communicate with, attempt to communicate with, store or alter data in, retrieve or remove data from, or otherwise make use of or attempt to make use of the logical, arithmetic, control, memory, storage, output, or communication functions of a computer, computer system, or computer network.

(j) "Computer hacking" means:

(1) accessing or attempting to access all or part of a computer, computer system, or a computer network without express or implied authorization for the purpose of establishing contact only;

(2) with the intent to defraud or with malicious intent to commit a crime after the contact is established;

(3) misusing computer or network services including, but not limited to, mail transfer programs, file transfer programs, proxy servers, and web servers by performing functions not authorized by the appropriate principal of the computer, computer system, or computer network. Misuse of computer and network services includes, but is not limited to, the unauthorized use of:

(i) mail transfer programs to send mail to persons other than the authorized users of that computer or computer network;

(ii) file transfer program proxy services or proxy servers to access other computers, computer systems, or computer networks; and

(iii) web servers to redirect users to other web pages or web servers;

(4) using a group of computer programs commonly known as "port scanners" or "probes" to intentionally access any computer, computer system, or computer network without the permission of the appropriate principal of the computer, computer system, or computer network. This group of computer programs includes, but is not limited to, those computer programs that use a computer network to access a computer, computer system, or another computer network to determine:

(i) the presence or types of computers or computer systems on a network;

(ii) the computer network's facilities and capabilities;

(iii) the availability of computer or network services;

(iv) the presence or versions of computer software including, but not limited to, operating systems, computer services, or computer contaminants;

(v) the presence of a known computer software deficiency that can be used to gain unauthorized access to a computer, computer system, or computer network; or

(vi) any other information about a computer, computer system, or computer network not necessary for the normal and lawful operation of the computer initiating the access.

This group of computer programs does not include standard computer software used for the normal operation, administration, management, and test of a computer, computer system, or computer network including, but not limited to, operating system services such as domain name services and mail transfer services, network monitoring and management computer software such as the computer programs commonly called "ping", "tcpdump", and "traceroute", and systems administration computer software such as the computer programs commonly known as "nslookup" and "whois". It is unlawful to intentionally and knowingly use such computer software to access any computer, computer system, or computer network to adversely affect computer or network access or performance; and

(5) the intentional use of a computer, computer system, or a computer network in a manner that exceeds any right or permission granted by the appropriate principal of the computer, computer system, or computer network.

Computer hacking does not include the introduction of a computer contaminant into a computer, computer system, computer program, or computer network.

(k) "Computer contaminant" means a computer program designed to modify, damage, destroy, disable, deny or degrade access to, allow unauthorized access to, functionally impair, record, or transmit information within a computer, computer system, or computer network without the express or implied consent of the owner. Computer contaminant includes, but is not limited to:

(1) a group of computer programs commonly known as "viruses" and "worms" that are self-replicating or self-propagating, and that are designed to contaminate other computer programs, compromise computer security, consume computer resources, modify, destroy, record, or transmit data, or disrupt the normal operation of the computer, computer system, or computer network;

(2) a group of computer programs commonly known as "Trojans" or "Trojan horses" that are not self-replicating or self-propagating, and that are designed to compromise computer security, consume computer resources, modify, destroy, record, or transmit data, or disrupt the normal operation of the computer, computer system, or computer network;

(3) a group of computer programs commonly known as "zombies" that are designed to use a computer without the knowledge and consent of the appropriate principal, and that are designed to send large quantities of data to a targeted computer network for the purpose of degrading the targeted computer's or network's performance, or denying access through the network to the targeted computer or network, resulting in what is commonly known as "Denial of Service" or "Distributed Denial of Service" attacks; or

(4) a group of computer programs commonly known as "trap doors", "back doors", or "root kits" that are designed to bypass standard authentication software, and that are designed to allow access to or use of a computer without the knowledge or consent of the appropriate principal.

(l) "Unauthorized access" means access of a computer, computer system, or computer network not explicitly or implicitly authorized by the appropriate principal of the computer, computer system, or computer network.

(m) "Unauthorized use" means the:

(i) use of a computer, computer system, or computer network not explicitly or implicitly authorized by the appropriate principal of the computer, computer system, or computer network;

(ii) the use of computer software not explicitly or implicitly authorized by the appropriate principal or licensee of the computer software; or

(iii) the authorized use of a computer, computer system, computer network, or computer software in a manner not explicitly or implicitly authorized by the appropriate principal or licensee.

SECTION 16-16-20. Computer crime offenses; penalties.

(1) It is unlawful for a person to wilfully, knowingly, maliciously, and without authorization or for an unauthorized purpose to:

(a) directly or indirectly access or cause to be accessed a computer, computer system, or computer network for the purpose of:

(i) devising or executing a scheme or artifice to defraud;

(ii) obtaining money, property, or services by means of false or fraudulent pretenses, representations, promises; or

(iii) committing any other crime.

(b) alter, damage, destroy, or modify a computer, computer system, computer network, computer software, computer program, or data contained in that computer, computer system, computer program, or computer network or introduce a computer contaminant into that computer, computer system, computer program, or computer network.

(2) A person is guilty of computer crime in the first degree if the amount of gain directly or indirectly derived from the offense made unlawful by subsection (1) or the loss directly or indirectly suffered by the victim exceeds ten thousand dollars. Computer crime in the first degree is a felony and, upon conviction, a person must be fined not more than fifty thousand dollars or imprisoned not more than five years, or both.

(3)(a) A person is guilty of computer crime in the second degree if the amount of gain directly or indirectly derived from the offense made unlawful by subsection (1) or the loss directly or indirectly suffered by the victim is greater than one thousand dollars but not more than ten thousand dollars.

(b) A person is also guilty of computer crime in the second degree where:

(i) he interferes with, causes to be interfered with, denies or causes to be denied any computer or network service to an authorized user of the computer or network service for the purpose of devising or executing any scheme or artifice to defraud, or obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises, or committing any other felony;

(ii) he deprives the owner of possession of, or takes, transfers, conceals, or retains possession of any computer, data, computer property, or computer-related property, including all parts of a computer, computer system, computer network, computer software, computer services, or information associated with a computer, whether in a tangible or intangible form; or

(iii) the gain derived from the offense made unlawful by subsection (1) or loss suffered by the victim cannot reasonably be ascertained.

(c) Computer crime in the second degree is a misdemeanor and, upon conviction for a first offense, a person must be fined not more than ten thousand dollars or imprisoned not more than one year, or both. Upon conviction for a second or subsequent offense, a person is guilty of a misdemeanor and must be fined not more than twenty thousand dollars or imprisoned not more than two years, or both.

(4) A person is guilty of computer crime in the third degree if the amount of gain directly or indirectly derived from the offense made unlawful by subsection (1) or the loss directly or indirectly suffered by the victim is not more than one thousand dollars. A person is also guilty of computer crime in the third degree if he wilfully, knowingly, and without authorization or for an unauthorized purpose engages in computer hacking. Computer crime in the third degree is a misdemeanor and, upon conviction for a first offense, a person must be fined not more than two hundred dollars or imprisoned not more than thirty days. Upon conviction for a second or subsequent offense, a person must be fined not more than two thousand dollars or imprisoned not more than two years, or both.

(5) Each computer, computer system, or computer network affected by the violation of this chapter constitutes a separate violation.

SECTION 16-16-25. Compensatory damages and restitution.

In addition to other civil remedies available, the owner or lessee of a computer, computer system, computer network, computer program, or data may bring a civil action against a person convicted under this chapter for compensatory damages, restitution, and attorney's fees. Compensatory damages and restitution may include:

(1) expenditures reasonably and necessarily incurred by the owner or lessee to verify whether a computer system, computer network, computer program, or data was altered, damaged, or deleted by the access;

(2) costs of repairing or, if necessary, replacing the affected computer, computer system, computer network, computer software, computer program, or data;

(3) lost profits for the period that the computer, computer system, computer network, computer software, computer program, or data was unusable; and

(4) costs of replacing or restoring the data lost or damaged as a result of a violation of this chapter.

SECTION 16-16-30. Venue.

For the purpose of venue under this chapter, a violation of this chapter is considered to have been committed in the county in which the violation took place; however, upon proper motion and the proper showing before a judge, venue may be transferred if justice would be better served by the transfer, to one of the following:

(1) a county in which an act was performed in furtherance of a transaction which violated this chapter;

(2) the county of the principal place of business in this State of the owner or lessee of a computer, computer system, computer network, or any part of it, which has been subject to the violation; or

(3) a county in which a violator had control or possession of proceeds of the violation or of books, records, documents, property, financial instruments, computer software, computer programs, or other materials or objects which were used in the furtherance of the violation.

SECTION 16-16-40. Applicability of other criminal law provisions.

The provisions of this chapter must not be construed to preclude the applicability of any other provision of the criminal law of this State, which presently applies or may in the future apply, to any transaction which violates this chapter.

6. SC 16-3-1040, Offenses against the person

SECTION 16-3-1040. Threatening life, person or family of public official or public employee; punishment.

(A) It is unlawful for a person knowingly and wilfully to deliver or convey to a public official or to a teacher or principal of an elementary or secondary school any letter or paper, writing, print, missive, document, or electronic communication or verbal or electronic communication which contains a threat to take the life of or to inflict bodily harm upon the public official, teacher, or principal, or members of his immediate family if the threat is directly related to the public official's, teacher's, or principal's professional responsibilities.

(B) It is unlawful for a person knowingly and wilfully to deliver or convey to a public employee a letter or paper, writing, print, missive, document, or electronic communication or verbal or electronic communication which contains a threat to take the life of or to inflict bodily harm upon the public employee or members of his immediate family if the threat is directly related to the public employee's official responsibilities.

(C) A person who violates the provisions of subsection (A), upon conviction, must be fined not more than five thousand dollars or imprisoned not more than five years, or both.

(D) A person who violates the provisions of subsection (B), upon conviction, must be fined not more than five hundred dollars or imprisoned not more than thirty days, or both.

(E) For purposes of this section:

(1) "Public official" means an elected or appointed official of the United States or of this State or of a county, municipality, or other political subdivision of this State.

(2) "Public employee" means a person employed by the State, a county, a municipality, a school district, or a political subdivision of this State, except that for purposes of this section, a "public employee" does not include a teacher or principal of an elementary or secondary school.

(3) "Immediate family" means the spouse, child, grandchild, mother, father, sister, or brother of the public official, teacher, principal, or public employee.

7. SC 16-17-430, Offenses against public policy

SECTION 16-17-430. Unlawful communication.

(A) It is unlawful for a person to:

(1) use in a telephonic communication or any other electronic means, any words or language of a profane, vulgar, lewd, lascivious, or an indecent nature, or to communicate or convey by telephonic or other electronic means an obscene, vulgar, indecent, profane, suggestive, or immoral message to another person;

(2) threaten in a telephonic communication or any other electronic means an unlawful act with the intent to coerce, intimidate, or harass another person;

(3) telephone or electronically contact another repeatedly, whether or not conversation ensues, for the purpose of annoying or harassing another person or his family;

(4) make a telephone call and intentionally fail to hang up or disengage the connection for the purpose of interfering with the telephone service of another;

(5) telephone or contact by electronic means another and make false statements concerning either the death or injury of a member of the family of the person who is telephoned or electronically contacted, with the intent to annoy, frighten, or terrify that person; or

(6) knowingly permit a telephone under his control to be used for any purpose prohibited by this section.

(B) A person who violates any provision of subsection (A) is guilty of a misdemeanor and, upon conviction, must be fined not less than one hundred dollars nor more than five hundred dollars or imprisoned not more than thirty days.