Descriptor Term: ACCEPTABLE USE OF ELECTRONIC TRANSMISSION CAPABILITIES
Descriptor Code: EFE-P
Date Issued October 30, 2003
Date Changed: June 26, 2008
September 30, 2009
May 1, 2012

1. Network Etiquette:

The use of technology requires that you abide by accepted rules of etiquette, which include, but are not limited to, the following:

a) Courtesy: Do not send or forward abusive messages to anyone.
b) Appropriate Content: Defamatory, intentionally inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing or illegal material is prohibited.
c) Privacy: All communication and information accessible via the network should be assumed to be copyrighted property. Transmission of data on the Internet cannot be guaranteed to be private or secure. Note that electronic mail (e-mail) is not guaranteed to be private. People who operate the system do have access to all mail and electronic transmissions. Electronic transmissions relating to, or in support of, illegal activities may be reported to the authorities. Do not reveal your or any individual's personal address, phone or credit card number.

2. Email

Limited personal use of email is permitted, however, personal use should not interfere with assigned duties and responsibilities. The use of email requires that you abide by accepted rules of etiquette, which include, but are not limited to, the following:

a) SPAM, the sending of unwanted mail is a significant problem for users and for the network. Do not send emails that are not directly business or school related to groups or persons within the system.
b) Using GCS email directories or address books to send emails that are for personal gain or that promise personal gain are a violation of Administrative Policy GAG
c) Use of GCS email directories or address books to communicate views, solicit membership, or raise funds for any non-school sponsored purpose, whether profit or non-profit, is prohibited.
d) Network administrators will distribute virus warnings. If you feel you have information regarding a virus please contact network administration immediately and do not forward such emails to users.
e) Email is not private. Technicians who operate the system can access all mail. Access is usually limited to investigative or trouble-shooting purposes, however, the Chief of Human Resources, Chief Information Officer, or the Superintendent may at any time, and for any reason, allow the search of email or data stored on all district owned computers.

3. **Passwords:** Passwords are personal and should not be shared with anyone. Attempts to log in to the system as any other user will result in cancellation of user privileges and/or criminal prosecution.

4. **Copyright:** Information transmitted through the Internet, which is copyrighted, is subject to the same copyright laws as govern non-electronic data.

5. **Security:** Security on any computer system is high priority, especially when the system involves many users. If you feel you can identify a security problem on the service provided you, notify a system administrator or teacher. Do not demonstrate the problem to other users.

6. **Plagiarism:** Data received through the Internet is subject to the same rules of documentation as traditional information. Give credit for all material used in research.

7. **Vandalism:** Vandalism will result in cancellation of your privileges. This includes, but is not limited to, altering web sites, intentionally damaging equipment or cabling, uploading or creation of a computer virus, and any other activity that corrupts individual programs, data or the network.

8. Network resources

The user is responsible for his or her actions and activities involving the network. Some examples of unacceptable uses are: wastefully using resources such as file space, file sharing networks, circumventing safety configurations, modifying setup policies, modifying settings on machines, attaching unauthorized devices, modifying infrastructure, invading the privacy of individuals, gaining unauthorized access to resources or entities, using the network while access privileges are suspended or revoked.

9. Unauthorized charges

The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges and/or equipment or line costs.

10. Warranties

GCS makes no warranties of any kind, whether expressed or implied, for the service it is providing. GCS will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed deliveries or service interruptions caused by its negligence or the users' errors, omissions, or failure to properly back up their data and files.

11a. Emerging Technologies

The tenets of Policy EFE are inclusive of emerging technologies in devices that provide wireless capabilities. Examples of these devices include, but are not limited to, mobile phones with cameras and personal digital devices with Internet connectivity.

Students and staff may bring their privately-owned electronic devices to use on Guilford County Schools' campuses. GCS retains the right to determine where and when personal devices may be connected to the network. There should be no expectation of privacy once they have connected to the district's computer system. There should be no expectation of network availability. Technology Services uses network appliances to control and monitor network access. Network access control

(NAC) tools may require users to authenticate (user name and password) and/or load required software (such as virus protection). The administration also reserves the right to determine if the use of the personal device is appropriate and/or disrupts the learning environment.

The following users are not permitted by students or staff on Guilford County Schools' campuses and school related activities:

a) Connecting to unfiltered Internet information,
b) Using such a device to capture images, transmit, and manipulate media electronically.

One example of an inappropriate use is using a camera phone to take pictures, emailing the pictures, or posting the pictures on the web.

Teachers and staff members that have devices capable of these functions are guided by the tenets of Policy EFE and are to ensure that no privacy rights are violated regarding the Family Education Rights Privacy Act (FERPA).
The use of technology resources and Internet access is a privilege and not a right; inappropriate use will result in cancellation of those privileges. Do not use the network in any way that will disrupt the use of the network by others. Technology Services may monitor all activity, log network usage, make decisions regarding whether or not a user has violated standards, policies or procedures; and may deny, revoke, or suspend access at any time.

11b. Web 2.0/Social Networking Tools:

Web 2.0/Social Networking Tools are a catch all phrase used to describe technology which integrates technology, social interaction and content creation. Limited use of Web 2.0/Social Networking Tools are permitted; however, personal use should not interfere with assigned duties and responsibilities.

Some examples are:

- Blogs
- Chat Rooms
- Podcasts
- Social Networking Sites
- Tweeting "Tweets"
- Virtual Worlds
- Wikis

Employees should familiarize themselves with GCS Code of Conduct found in the **Personnel Handbook** and other guidelines/resources (such as the Social Media Guidelines) posted on the Guilford County Schools' web site that provide direction for employees participating in online social media activities. The use of Web 2.0/Social Networking Tools requires that you abide by acceptable rules of etiquette. The following conducts are discouraged:

- Engaging in vulgar or abusive language, personal attacks, or offensive terms targeting individual and/or groups
- Endorsement of commercial products, services, or entities
- Endorsement of political parties, candidates, or groups

- Lobbying members of any elected body using resources of GCS

Issues to be aware of:

- Items published on the web are persistent. You should consider all items published on the web to be public domain.
- When discussing item(s) involving GCS or GCS related matters you may wish to contact the District Relations Department prior to publishing content.
- Per the State of North Carolina guidelines for school system employees, you must maintain an appropriate relationship with students in all settings.
- Access to social media must be closely monitored to ensure that it is appropriate for student use. The educator is solely responsible for the content they allow students to view.
- When posting to web sites outside of GCS you may wish to include a disclaimer such as, "The views expressed in this post are not those of Guilford County Schools."
- Do not reference your position within the GCS system when writing in a nonofficial capacity.
- Respect copyright laws.
- Make sure your online presence reflects how you wish to be seen by the public as a GCS Professional.
- Have no expectation of privacy.

12. **Internet Safety and Children's Internet Protection Act (CIPA) and Guilford County Schools Student Email Accounts**. The Children's Internet Protection Act (CIPA), enacted December 21, 2000, requires that recipients (Guilford Country Schools) of federal technology funds comply with certain Internet filtering and policy requirements.

Access to Inappropriate Material

- To the extent practical and feasible, technology protection measures (or "Internet filters") are used to block or filter Internet traffic, and other forms of electronic communications (student email). Access to inappropriate information as required by the Children's Internet Protection Act, will be filtered or blocked. This is applied to visual depictions of material deemed obscene, child pornography, or to any material deemed harmful to minors.

Inappropriate Network Usage

- To the extent practical and feasible, technology measures and policies are used to promote the safety and security of users of the online computer networks, while using electronic mail, and other forms of direct electronic communications. Inappropriate network usage includes, but is not limited to:
  a) unauthorized access, including so-called 'hacking', and other unlawful activities
  b) unauthorized disclosure, use, and dissemination of personal identification information regarding students
  c) using another student's user name and password to access network resources
  d) transmitting obscene or pornographic visual imagery

e) harassing, menacing, any type of language that is deemed profane, cyberbullying, threatening or communication that indicates fear or intimation to an individual or groups of individuals.

Education, Supervision and Monitoring

While GCS takes considerable steps to electronically block inappropriate materials and sites, it is the responsibility of all district school staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet.

- Students, teachers and staff members will be informed of the intent of the Acceptable Use Policy by its inclusion in the Student Handbook and Personnel Handbook.
- The district will provide teachers, students and parents with guidelines and various computerized informational resources for the protection of students while using technology. The resources will be age-appropriate and designed to promote student safety with regard to Internet usage. This includes lessons on cyberbullying, appropriate online interactions and the use of social networking sites.
- Cyberbullying is the act of bullying or harassment through the use of any electronic means. Any form of cyberbullying is strictly prohibited and will result in appropriate disciplinary action. Students should promptly disclose to their teacher or other school official any inappropriate, threatening, or unwelcomed message (as outlined in District Policy JCDAD).
- Technology Services for Guilford County Schools will supervise and monitor usage of district resources, the network infrastructure, and access to the Internet in accordance with this Policy and the Children's Internet Protection Act. Any use of an electronic medium connected to these resources (an example is, but not limited to; student email accounts) is governed by this Policy.
- Anyone found violating tenets of Policy EFE, the Children's Internet Protection Act (CIPA) or Guilford County Schools Student Email Accounts provision will have their access revoked and will be subject to the actions defined in the Student Code of Conduct.
- Procedures for the disabling or otherwise modifying of any technology protection measures shall be the responsibility of Guilford County Schools Technology Services or designated representatives.