



McDonough, Georgia

Three-Year Technology Plan

July 1, 2011 – June 30, 2014

Submitted to the Georgia Department of Education
April 2011

Superintendent
Henry County Schools
Dr. Ethan Hildreth

Director of Technology Services
Henry County Schools
Mr. Scott Pierce

Coordinator/Operations Analyst
Georgia Department of Education
Mr. Charlie Jackson

Table of Contents

I. Vision for Technology Use	3
II. Current Reality	4
Data Sources	4
Instructional Technology Use	4
Instructional Gap Analysis	6
Administrative Technology Use	6
Administrative Gap Analysis	7
Parent/Community Uses of Technology	7
Parent/Community Gap Analysis	7
Goals, Benchmarks, and Strategies	8
III. Communication and Marketing	13
IV. Professional Development	13
Appendix	15
Strategy Alignment with School System Initiatives	15
Web Site Posting Guidelines	16
Board Policy Electronic Communications	17
Authorized User Policy	27

I. Vision for Technology Use

The mission of Henry County Schools is to be “committed to ensuring educational success for each student.” The district’s vision is to move from good (ensuring each student meets or exceeds grade-level performance standards) to great (ensuring each student graduates high school prepared for further learning). Henry County Schools believes that technology is not what drives school improvement but is a tool that enables and accelerates it. Our vision is to provide, assist and support stakeholders in their use of technology to achieve our commitment of ensuring success through greater flexibility, increased productivity, increased support of standards-based instruction, improved response to accountability, and expanded opportunities for student learning, professional development, communication and feedback.

II. Current Reality

Data Sources

The following sources of data are used by Henry County Schools to inform technology planning decisions:

- Student assessment data
- Henry County Schools Balanced Score Card
- Individual school improvement plans
- Annual Technology Inventory submitted to the Georgia Department of Education
- Annual Henry County Schools Technology Services budget
- Annual Perception Survey
 - Students
 - Staff
 - Parents/Community
- Annual Technology Utilization Reports
 - Monitor internet activity
 - Infrastructure resources
- Online curricular resource reports
- GaDOE Statewide Longitudinal Data System

Instructional Technology Use

All Schools

Each school in Henry County is equipped with a common collection of instructional software, hardware, and online resources which includes:

- GraphClub
- Microsoft Office Suite
- netTrekker

- OpenMind graphic organization software
- Interactive Technology cart
- Instructional response units (eInstruction, ActiVote, Turning Point)
- Teacher instructional Web pages
- A learning management system
- A benchmark assessment system

Each school in the district is networked with Metro-E. The local area network provides network connectivity to all classrooms (permanent and modular), computer labs, library media centers, and other instructional areas.

High speed internet access is available to each network connection. Internet service is provided by AT&T and Cogent. Each school has been provided at least two instructional computers per classroom and the student to computer ratio is approximately 3 to 1.

Each school is provided access to a common (union) instructional resource management and circulation system. Schools also utilize a web-based electronic grade book program via the student information system.

An instructional technology coordinator and four instructional technology specialists are responsible for designing and implementing technology related and media services related professional learning and training. The library media program is supported by at least one certified library media specialist in each school. Each high school employs a full time media center paraprofessional. Middle schools and elementary schools employ a half time media paraprofessional.

Elementary Schools

Each elementary school has one computer lab and a library media center with multiple research stations. In addition to the software mentioned in the All Schools section (above), elementary schools utilize the Accelerated Reader program and computer labs are equipped with STAR Reading.

Middle Schools

Middle schools each utilize at least one stationary computer lab, one Business Education lab, and have a minimum of two wireless laptop carts. Each middle school uses the My Access writing program at either the seventh or eighth grade level and the Academy of Reading and Academy of Math programs, and the KeyTrain program at all levels.

High Schools

Each of the ten high schools has at least one flexibly scheduled stationary computer lab and a minimum of two wireless laptop carts. In addition to the software mentioned in the All Schools section above, high school computer labs also provide Geometer's Sketchpad, the Wilson Web Biography Reference Bank, and the KeyTrain program. High

school library media centers also provide access to the Wilson Web resource. The Career Technology and Agriculture Education program also supports computer labs at each high school that are dedicated to their respective programs. Additionally, the Academy of Reading and Academy of Math programs are available to students in any of the high school computer labs and the Angel Learning online learning management system is utilized for online and blended learning opportunities for students.

Non Systemic Technology

Henry County Schools encourages local (school-based) funding of technology that enables best instructional practices. The district supports the acquisition, training, and implementation of such technologies. To this extent, the district identifies a number of research-based solutions from which schools can choose and provides support to schools that acquire these technologies. Such technologies include a learning management system, interactive whiteboards and tablets, online instructional resources, learner response systems, and document cameras.

Instructional Gap Analysis

An analysis of data sources and an examination of current instructional technology use reveal areas of concentration to better achieve the vision for technology use. Of particular interest is that certain technology resources are underutilized. Examples of such resources include the learning management system and the assessment management system. There is a need to better utilize these technology resources.

Student access to technology in the classroom and in computer labs continues to be an area of interest including access to non computer resources such as interactive white board technologies, learner response systems, and document cameras. Student access to such technologies is limited as is student access to online collaboration and communication tools due to filtering limitations and available resources. Improved access to curricular resources is needed for both students and parents both at home and at school.

There is a need for increased opportunities for online learning, blended learning, and online/blended professional learning. Expanded use of the district web presence for communication and feedback is also needed as is a universal diagnostic student screening tool.

Administrative Technology Use

The Technology Services department, manages, and supports most administrative technologies centrally. The department supports every other department within the school district including Learning and Teaching Services, Human Resource Services, Financial Services, Leadership Services, Administrative Services, and each of the district's 51 schools.

Faculty and administration are provided network access with email and student information system availability both at home and school. Sharepoint is also available as a central electronic document management, communications, and intranet platform and the Microsoft Office suite is available to all system network users. Infinite Campus is used as the district's student information system. This system incorporates many processes and applications which previously operated separately. The district's attendance program, grade book program, student Individualized Education Program system, scheduling system, school nutrition application system, parent connection tool, and other essential services are incorporated into the student information system. The district complies with both the Children's Internet Protection Act and the Family Educational Rights and Privacy Act.

Administrative Gap Analysis

Providing Internet bandwidth sufficient to meet growing demand is a continuing challenge for Henry County Schools. While the state bandwidth allotment is currently insufficient to meet the needs of our schools, the district has provided local funds to supplement this allotment for the current budget cycle. However, the continuation of sufficient bandwidth will be necessary as demand increases.

As demand increases for data to be housed in systems that are accessible to larger numbers of people, a solution is needed that will better provide data to stakeholders who need to access and translate data into more usable forms.

A tool for collecting administrative evaluation of teacher performance is needed. A tracking system for the evaluation of our existing and ongoing use of technology is also needed.

Parent/Community Uses of Technology

The school system utilizes email, website, phone, and online survey technologies and limited social networking tools in an attempt to provide effective communication with all stakeholders. Infinite Campus Parent Portal is an online tool for school staff to use to communicate information relating to grades, assignments, handouts and other communication relevant to parents. Parents and teachers can communicate via email and an automated phone calling system is optionally available at schools.

Some schools provide afterhours access to computers in library media centers and computer labs.

Parent/Community Gap Analysis

No system wide communication tool is currently available for all parents and students. While Infinite Campus Parent Portal provides communication to parents and students, it is only used at the middle and high school levels. Elementary schools currently do not use a system wide platform for parent and student communication.

Emergency alerts to parents and the community are currently limited to a web page posting on the system website. No district wide program currently exists to send such information out via email, phone, SMS, or other types of electronic communication.

Although some schools provide afterhours access to computers in library media centers and computer labs, such programs are informal and occur on a limited basis. A system for online academic resources is not currently available to parents and the community.

Goals, Benchmarks, and Strategies

Goal 1: Expanding online learning opportunities for staff and students				
Strategies	Benchmarks	Evaluation	Funding Source	Responsibility
1A: Increase online Course offerings and course content.	<ul style="list-style-type: none"> •Continue to expand online course offerings through Henry County Online Academy for 2011 – 2014. •Provide online course content to all core content high school teachers for use with students •Increase selection of online courses 	<ul style="list-style-type: none"> •Collect and analyze growth in online enrollment data • Periodic analysis of instructional content in the learning management system (LMS) to inform the level of content development 	Local funds	Instructional Technology Coordinator Curriculum Coordinators
1B: Increase selection of online courses for technology related online and blended professional learning and training for	<ul style="list-style-type: none"> •Increased online and blended professional learning offerings for 	Examine learning management system usage by teachers and students	State and local funds	Instructional Technology Coordinator Instructional

classified, certified, and administrative staff.	2011 – 2014 through Dell Learn and Angel course content. •			Technology Specialists
1C: Increase online collaboration	Provide collaborative tools to all teachers and students	Collect and analyze data associated with online collaboration tools	No additional funds needed	Instructional Technology Coordinator Information Systems Coordinator
Goal 2: Better accommodate best practices in student assessment and data analysis				
Strategies	Benchmarks	Evaluation	Funding Source	Responsibility
2A: Provide tools and professional learning to improve the use of data to inform instruction.	More frequent processing of student data within the assessment management system. Increased professional learning opportunities related to the use of data to inform instruction via the student information system and the Statewide Longitudinal Data System.	Instructor use of SIS for student assessment data and instructor use of SLDS	No additional funds necessary	Data Management Coordinator Instructional Technology Coordinator Instructional Technology Specialists
2B: Expand and support balanced assessment of student learning	Provide professional learning in support of diagnostic, formative and/or	Number of teachers and administrators served with professional learning.	Local funds	Instructional Technology Coordinator

	common, and summative assessment			
2C: Utilize the district's student information system to better inform instructional, financial, and organizational decisions.	<ul style="list-style-type: none"> •Provide professional learning in the most effective way to use the student information system (SIS) to inform practice •Expand support for SIS 	<ul style="list-style-type: none"> •Collect data related to the number of stakeholders served. •Collect related perception data to ensure that stakeholder needs are met 	Technology Services budget via local funds	Data Management Coordinator Information Systems Coordinator Instructional Technology Coordinator
Goal 3: Provide resources to meet student and school needs				
Strategies	Benchmarks	Evaluation	Funding Source	Responsibility
3A: E-rate applications will be filed to apply for discounted rates for WAN connectivity, cellular connectivity, and the district's phone system.	E-rate applications will be filed annually for any eligible services.	Annual technology budget	Eligible E-rate awards excluding end-user equipment. Amount: Awards contingent upon USAC	Director of Technology Services
3B: Provide standardized equipment and resources that support best instructional practices in classrooms	<ul style="list-style-type: none"> •WAN connectivity to all schools •Acquire relevant technology for schools 	Determine whether connectivity and tools are in place	Local Funds SPLOST	Director of Technology Services Network Coordinator Instructional Technology Coordinator
3C: Provide student and teacher access to curricular resources and productivity tools	District will increase electronic curricular resources and	Perception surveys	Local funds	Director of Technology Services Information

	<p>improve accessibility to these resources.</p> <p>Teachers will continue to develop curricular resources for blended learning classes.</p>			<p>Systems Coordinator</p> <p>Network Coordinator</p> <p>Instructional Technology Coordinator</p> <p>Data Management Coordinator</p>
3D: Utilize the district web content management system for instruction, communication, and feedback	Each school, department, and teacher develops and maintains a web presence.	Analyze web authoring analytical	No additional funding needed	<p>Director of Technology Services</p> <p>Instructional Technology Coordinator</p> <p>Instructional Technology Specialists</p> <p>Library Media Specialists</p>
3E: Provide a district wide wireless connectivity solution	Wireless connectivity for each classroom and commons areas within schools	Wireless equipment installed in each school.	SPLOST	<p>Director of Technology Services</p> <p>Network Coordinator</p>
Goal 4: Supporting best practices of instruction through professional learning				
Strategies	Benchmarks	Evaluation	Funding Source	Responsibility

4: Provide a menu of technology related professional learning from which schools can choose and deliver professional learning based on school improvement needs	Menu is finalized and published for school administrators' and district use	Completed technology related professional learning courses and training reflect support for best instructional practices through technology integration	Local funds	Instructional Technology Coordinator Instructional Technology Specialists Library Media Specialists Technology Contact Teachers
Goal 5: Community and parent access				
Strategies	Benchmarks	Evaluation	Funding Source	Responsibility
5A: Improve parent access to student progress and performance data (via Campus Portal)	<ul style="list-style-type: none"> •All ES, MS, & HS parents and students have access to student progress and performance •Parents notified of access to progress and performance data 	Monitor number of activated accounts in Campus Portal	Local Funds	Information Systems Coordinator
5B: Improve and expand parent and community access to academic resources	District will expand access to electronic curricular resources	Perception surveys	Local funds	Director of Technology Services Executive Assistant Network Coordinator Instructional Technology Coordinator

				Information Systems Coordinator
--	--	--	--	---------------------------------------

III. Communication and Marketing

The Administrative Services department assists in disseminating information to the media and community. The office works with local and metro news contacts and utilizes a variety of communications media including the system website and various social networks. These communication systems provide important information to parents and the community including the district's vision, mission and goals. They feature information of general interest to parent and community stakeholders as well as a breaking news page, information for public review, the school calendar, recognitions, lunch menus, upcoming events, and specific information about the district. School websites are also used to communicate school specific information and provide sections related to academics, activities, administration, athletics, general information, and the school calendar. Additionally, school websites feature teacher pages that allow teachers to create parent/teacher and student/teacher communication as well as classroom related instructional web pages. The instructional pages provide teachers a method in which to extend the classroom beyond the walls of the schools and help to support teachers' standards-based instruction.

Infinite Campus Parent Portal is an online tool for school staff to use to communicate information relating to grades, assignments, handouts and other information relevant to parents. This system is also used to disseminate information to parents who subscribe to the email distribution feature. Administrators or teachers can send out information to all enrolled users or can target messages to specific groups such as a particular class. Schools may also utilize electronic communication system to communicate information to parents and students.

The Technology Services department holds periodic meetings with school administrators, instructional technology and other school technology contact persons to provide these stakeholders a channel of communication with the department. The meetings typically begin by providing updates on specific topics and projects but also focus on addressing general questions and concerns from the school. The department also meets regularly with the district's leadership team.

IV. Professional Development

The philosophy of the Technology Services department regarding instructional technology related professional learning is to focus first on the standards-based instruction that technology is supporting and then to concentrate on how technology can enable and accelerate this instruction. To this end, the department plans to expand on a series of courses that focus on supporting standards-based instructional best practices with technology. The district utilizes an instructional technology coordinator and four instructional technology specialists who deliver this professional learning in schools. A menu of technology related professional learning is provided from which administrators can choose to meet the needs of their school's continuous improvement plan. Some professional learning is provided in an online learning environment or in a blended online/face-to-face environment. Online and blended professional learning will be consistent with iNacol's National Standards of Quality for Online Courses and the International Society for Technology in Education's NETS standards. Professional workshops and conferences are also a part of technology related professional learning. The district provides funding to send instructional technology personnel, Technology Services personnel and other staff to professional learning workshops and conferences. Members of the technology services department, the instructional technology coordinator, and instructional technology specialists attend the Georgia Educational Technology Conference (GaETC). GaETC provides numerous concurrent sessions, workshops, and poster sessions specific to educational technology. Technology Services staff members attend the following professional learning opportunities:

- Georgia Student Information Systems Conference
- GAMIS
- GaDOE Data Collection Workshops
- Infinite Campus Interchange
- Microsoft Professional Training
- Various vendor training opportunities

An expanding professional resource library is also a part of the professional learning plan. Resources related to instructional technology and standards-based instructional best practices are available for staff to check out from the department. Example titles include *Differentiating Instruction with Technology in K-5 Classrooms* and *Using Technology with Classroom Instruction That Works*.

Funding sources for technology related professional development come from both local and state sources.

Appendix

Alignment with Henry County Schools Strategic Plan 2011-2016

SA: Student Achievement	CCC: Culture, Climate & Community	QA: Quality Assurance
-------------------------	-----------------------------------	-----------------------

	SA	CCC	QA
Strategy 1A	✓	✓	✓
Strategy 1B	✓		✓
Strategy 1C	✓	✓	
Strategy 2A	✓		✓
Strategy 2B	✓		✓
Strategy 2C	✓	✓	
Strategy 3A	✓	✓	
Strategy 3B	✓	✓	
Strategy 3C	✓	✓	
Strategy 3D	✓	✓	
Strategy 3E	✓	✓	
Strategy 4			✓
Strategy 5A	✓	✓	
Strategy 5B	✓	✓	

Henry County Schools Communication Guidelines

Web Page Posting

- 1) Schoolwires is Henry County Schools (HCS) web page authoring solution.
- 2) Individual school web sites will originate from and be housed in the school system Data Center. All school system related web sites will be hosted by HCS.
- 3) All web page content developed for HCS becomes the property of HCS.
- 4) A school web site coordinator will be designated to coordinate the web site (including school, teacher, and extracurricular organizational web pages).
- 5) The principal at the individual school or the principal's designee is recommended to designate a school Web page review committee. It is recommended that the committee be composed of a building level administrator, a representative from each grade level or subject area, the Web Coordinator and the media specialist.

- 6) With the approval of the principal or the principal's designee, extracurricular organizations may create and maintain web pages within the school web site. Extracurricular organizations include, but are not limited to, school sports teams, bands, orchestras, PTO/PTSOs, cheerleading teams, and other extracurricular activities. Web sites for external groups (such as booster clubs) will not be linked to the school web site. HCS is not responsible for the content of web sites that are not hosted in the school system web page authoring solution.
- 7) HCS reserves the right to remove material from all web pages including teacher, student or extracurricular organization web pages. This includes removal of the web pages in their entirety when the material does not fall within the school system communication guidelines or board policy.
- 8) Web pages may not contain copyrighted material unless prior written permission is obtained. Copyrighted material will be properly cited using a standard citation format.
- 9) A current list of Partners-in-Education (with logos and contact information) is permitted along with a link to the Partners-in-Education's Web site(s). School system web pages will not include links to other commercial businesses or advertisements and will not solicit business, advertise, or otherwise engage in commercial enterprise.
- 10) The capability of web links to pass through the school system web content filter will be verified prior to posting.
- 11) All content posted to HCS web pages will adhere to the Acceptable Use Policy as well as the Electronic Use Policy (IFGBA).
- 13) For all classroom/ activity web pages that are identified as being exclusive to students with disabilities, it is required that permission from each student's parent(s) be obtained prior to that student's name, picture, or video being posted. Although a student's picture may appear on the school webpage, children should not be identified on any web page as students with disabilities without parental consent. If a student's name, photo, or video appear without being identified as a student with disability, no parental consent is required.
- 15) Each teacher will provide, at a minimum, their HCS e-mail address and an introduction on their faculty web page.
- 16) Web pages should be reviewed regularly to ensure the content is current and accurate.

Expectations for Communicating Electronically

Henry County Schools (HCS) recognizes that today's students and parents engage in electronic forms of communication for their daily interactions with friends, family, and their larger social networks. HCS too has turned to e-mail, websites, blogs, text messaging, and use of public social media networks such as Twitter, Facebook, and others to communicate with similar groups. Whereas these forms of communications are dynamic, mobile, and quickly reach their audience through technologies that have become an integral part of our online lives, they may, in some circumstances, not meet the public and professional standards for communicating with students and parents.

It is important to create an atmosphere of trust and individual accountability when communicating electronically keeping in mind that information produced by HCS employees is a reflection on the entire district. By accessing, creating or contributing to any blogs, wikis, or other social media for classroom or district use, you agree to abide by these expectations. Please read them carefully before posting or commenting on any blog or creating any classroom blog, wiki and/or podcast.

HCS will maintain an official social media presence using sites such as Facebook and Twitter for the district and for each school. These official pages will be designated with logos and language to maintain the branding of the schools and the system.

Non-District email, instant messaging and texting from personal accounts to communicate with students or parents about school matters is considered an unacceptable communication method.

Employees should not use their District email address or phone number for communications on social media networks for personal accounts. Communications between public educators students and parents should always be transparent, accessible and professional.

All employees must adhere to the Georgia Code of Ethics for Educators (<http://www.gapsc.com/Rules/Current/Ethics/505-6-.01.pdf>).

The Henry County Schools (HCS) provides employees appropriate electronic access, consisting of e-mail communication, network connectivity, student information system (SIS) and fund accounting system (FA) access where appropriate, and Internet/World Wide Web access. This policy governs the use of HCS electronic resources at HCS sites to include but is not limited to Internet, World Wide Web (WWW), chat rooms, electronic mail, data, online resources, online services, portable media, network information, licensed software, telecommunication resources, HCS Intranet and all other school system electronic messaging systems and data systems. This policy covers the use of electronic communication, network, software, hardware, and related HCS services. Violations of the electronic Communications policy *may cause an employee's or student's access privileges to be revoked, School Board disciplinary action and/or appropriate legal action may be taken, up to and including termination of employment.*

I. E-MAIL

HCS e-mail system is designed to provide electronic communication and use of related resources. Employees or students with e-mail access shall adhere to the following procedures:

- a. Email accounts are provided for employees and/or students only.
- b. Email accounts are provided for professional and academic purposes. Email accounts should not be used for personal gain, personal business activities or to solicit for non-school system business; broadcasting of unsolicited messages is prohibited.
- c. The HCS provided email account should be used for all school related business. Personal email accounts should not be used.
- d. All electronic communication created, sent or received via HCS e-mail system is the property of HCS. Employees shall not have any expectation of privacy regarding this information. HCS reserves the right, as needed, to access, read, review, monitor and copy all messages and files on its computer system without notice. When deemed necessary, HCS reserves the right to disclose text, video, audio or images files to law enforcement agencies without the employee's consent.
- e. Staff and students shall use caution to ensure that the correct e-mail address is used for the intended recipient(s).
- f. Alternate Internet Service Providers (ISP) or anonymous connections are not permitted unless expressly authorized by HCS and properly protected by a firewall or other appropriate security device(s).
- g. Only authorized administrative personnel are permitted to access another user's e-mail without consent.
- h. Employees shall exercise sound judgment when distributing messages. Student related messages should be guarded and protected. Employees must abide by copyright laws, ethics rules and applicable state and federal laws.
- i. E-mail messages should only contain professional and appropriate language. Employees shall not send abusive, harassing, intimidating, threatening, discriminatory or otherwise offensive messages.
- j. Spam messages, messages containing Malware, inappropriate graphics and/or executable programs shall be deleted.
- k. Employees shall archive messages regularly to prevent exceeding limits for e-mail storage.
- l. Human Resources via board agenda shall report all changes in worker duties or employment status to Technology Services. Such changes include termination of employment, lateral moves or any job change that would require an update of network/e-mail account information or a change in network/e-mail access.
- m. E-mail access for retiring HCS employees or employees leaving the school system shall be disabled and/or deleted on the last day of employment.
- n. Access to e-mail accounts under investigation shall be restricted without notice until authorized by the Superintendent or designee.
- o. While HCS encourages respect for the rights and sensibilities of others, it cannot protect individuals against the existence or receipt of materials that may be offensive to them. Those who make use of electronic communications may come across or be recipients of material that they might find offensive or annoying. In such cases where materials are received, the users shall delete the non-school system business related content. HCS is not responsible for the views expressed by individual users via web pages, electronic mail or other on-line communications.

II. NETWORK

a. Personal Responsibility: By accepting an account password, related information, and accessing HCS network, intranet or internet system, an employee agrees to adhere to HCS policies regarding their use. Employees should report misuse or policy violation(s) to administration or Director of Technology Services.

b. Permitted Use and Terms: Use of HCS network and the internet is a privilege, not a right. Use of network, intranet and internet access extends throughout an employee's term of employment, providing the employee does not violate HCS policy.

c. Availability and Access: The Superintendent, at their discretion has the right to suspend access at any time, without notice for possible HCS policy violations, security or administrative concerns. The Director of Technology Services shall have the right to suspend network access at any time, without notice, for technical reasons or possible violation of state and federal laws.

i. Network access for retiring HCS employees or employees leaving the school system shall be disabled and/or deleted on the last day of employment.

ii. Fund accounting and student information system access for retiring HCS employees or employees leaving the school system shall be disabled and/or deleted on the last day of employment.

iii. Access to network accounts under investigation shall be restricted without notice until authorized by the Superintendent or designee.

d. Privacy: Network and Internet access is provided as a tool for school system related business. HCS reserves the right to monitor, inspect, copy, review, and store at any time, without prior notice, any and all usage of the network and the internet. This includes, but is not limited to, all materials, files, information, software, communications, and other content transmitted, received, or stored in connection with this usage. All such information, content, and files are the property of HCS. An employee should have no expectation of privacy regarding such information.

e. Downloaded Files: Employees are reminded that information obtained from the Internet or externally connected device is not always reliable and should be verified for accuracy before use. Any files downloaded from the Internet must be scanned with school system virus detection software before being opened.

i. All HCS related files should be stored on system provided resources. Offline storage or web hosting services should not be utilized for HCS related documentation.

f. Confidential Information: Employees may have access to staff or student information that is considered confidential as related to their job responsibilities. Employees may use e-mail to communicate confidential information internally to those with a need to know. Such e-mail shall be marked "Confidential." For purposes of this policy, confidential information is defined as:

i. Procedures for computer access and passwords of HCS users, program manuals, user manuals, or other documentation, screen, file, or database layouts, systems flowcharts, and all documentation normally related to the design or implementation of any computer programs developed by HCS relating to computer programs or systems installed for internal use.

ii. Lists of information about personnel seeking employment with or who are employed by HCS.

iii. Information relating to HCS's research, development, purchasing and marketing.

iv. Transmission of information that is confidential under HCS policy, state or federal law or regulations.

g. Physical Security: The following policies are designed to effectively maximize technology resources, maintain the integrity of the school system and protect HCS's assets. Employees shall adhere to the following:

i. Do not keep liquids or magnets on or near the computer.

ii. Do not remove a computer from a room/building without permission from Technology Services.

iii. Minimize transportation of portable media such as CD's, external hard drives and jump drives back and forth between home and school system sites. This will assist with minimizing school system exposure to viruses.

It is expected that there will be instances where lesson plans, word processing documents, spreadsheets, electronically created presentations, etc., are required to be used, reviewed, and graded from home. In those situations, files must be scanned on an updated school system antivirus scanner prior to use on the HCS network.

iv. Computing equipment shall be placed in an environmentally controlled location (e.g., temperature control, humidity, exposure to water, etc.)

v. Critical computing resources and equipment such as core switches, routers, and servers must be stored in secure locations.

vi. Magnetic media such as hard disk drives, external hard drives, or tapes must be formatted before disposal.

vii. A shredder shall be used for the disposal of sensitive documents.

viii. An UPS (Uninterrupted Power Supply) is required for all critical networking devices and servers.

ix. Critical/Confidential data, or a copy of it, shall not be stored on a computer or offline storage to include laptops, handheld devices external hard drives, jump drives, or any other mobile device.

Critical/confidential data is defined as data that cannot be replaced should it be lost or stolen or data that would cause financial harm or other hardship to the HCS should it become public. This type of information includes financial data, personnel files, password lists, program manuals, operating guides, encryption keys, decompiled HCS programs, student information or any other software, manual or data component deemed critical in nature.

x. All hardware that has been replaced, upgraded or is no longer usable should be immediately removed and/or disposed of properly.

III. SOFTWARE

Software piracy is both a crime, and a violation of HCS's Electronic Communications Policy.

Employees shall use software strictly in accordance with its license agreement. Unless otherwise provided in the license, the duplication of copyrighted software (except for backup and archival purposes by designated administrative personnel) is a violation of copyright law.

To ensure compliance with software license agreements and HCS's Electronic Communications Policy, employees shall adhere to the following:

a. Employees shall use software in accordance with the manufacturer's license agreements and HCS's Software Usage Policy. HCS licenses the use of computer software from a variety of outside companies. HCS does not own the copyright to software licensed from other companies. Employees are placed on notice that they do not own software or its related documentation.

b. HCS does not condone, and prohibits, the unauthorized duplication of software. Employees illegally reproducing software shall be subject to disciplinary action. Employees illegally reproducing software may be subject to civil and criminal penalties including fines and imprisonment.

c. Any employee, who knowingly makes, acquires, or uses unauthorized copies of computer software licensed to HCS, or who places or uses unauthorized software on HCS's premises or equipment, shall be subject to disciplinary action.

d. Employees shall not install personal software on HCS computers.

e. Employees shall not copy software from HCS's computer system for installation on home or other computers without prior authorization from the Director of Technology Services.

f. In unique cases that require an employee to use software at home HCS will purchase an additional copy or license. Any employee issued additional copy(s) of software for home use acknowledges that such additional copy(s) or license(s) purchased for home use are the property of the HCS. Employees who are required to use software at home shall contact the Director of Technology Services or school Administrator or appropriate department that maintains the license to determine if appropriate for home use.

- g. Employees who suspect or become aware of software misuse shall notify school administration or Director of Technology Services.
- h. No technology software purchases can be made except through HCS purchasing procedures. The Director of Technology Services shall be contacted prior to purchase.
- i. Freeware, third-party software, or any other type of software, obtained, downloaded or purchased is prohibited from being loaded on any HCS system without the permission of the Director of Technology Services. This includes, but is not limited to: screen savers, games, weather software, flash or java cartoons/games/modules, FTP software, remote control software, key loggers, sniffers, music players, file sharing applications or any other software or component that has the potential to modify the system from its standard HCS operating system configuration.
- j. Software and applications shall be approved by the Director of Technology Services as part of a pre-deployment research and development phase. Failure to submit to a pre-deployment research and development phase request may result in removal of the software or application, or service in question, or may delay the rollout of the application or service.

IV. HARDWARE

This section of the Network Security Policy is to define standards to be met by all equipment owned, leased and/or operated by Henry County Schools. Devices or equipment that are Internet facing and outside the HCS firewall are considered part of the “demilitarized zone” (DMZ) and are also subject to this policy.

This policy covers any host device outsourced or hosted at or by external/third-party service providers if that equipment resides with a system site.

All new equipment which falls under the scope of this policy must be configured according to the standards as set forth by Technology Services. All existing and future equipment deployed on HCS networks must comply with this policy.

- a. The following information must be documented or provided for all vendor provided equipment.
 - i. Host contact(s) and location of equipment
 - ii. Specific hardware configuration documentation showing operating system and/or firmware version.
 - iii. Main functions and applications
 - iv. Password groups for privileged passwords and/or administrative access logins.
- b. Network interfaces must have appropriate Domain Name Server (DNS) records.
- c. For third party or outsourced equipment or applications, access to equipment and system logs shall be granted to members of HCS Technology Services upon request. Failure to grant these requests in a timely manner may result in the removal of the equipment or application in question.
- d. Hardware, operating systems, services, and applications shall be approved by Technology Services as part of a pre-deployment research and development phase. Failure to submit to a pre-deployment research and development phase shall result in removal of the equipment, application, or service in question, or may delay the rollout of new equipment, application, or service.
- e. Employee and/or student personal hardware shall not be connected to the school system network unless approved by Technology Services. HCS will not be responsible for the consequences of such actions.
- f. Changes to existing equipment must be preceded by written notification to the Director of Technology Services. The Principal shall take no action until the Superintendent or the Director of Technology services communicates approval in writing.
- g. System configurations shall be done according to the HCS Technology Services standards.
- h. Application services not required by HCS Technology Services, or by the local application, must be disabled.
- i. Remote administration, remote connection, terminal services, and Virtual Private Network (VPN) is prohibited for general users and may not be used, except by prior permission of Technology Services.

- j. Security-related logs or audit trail logs may be used or reviewed by Superintendent or Director of Technology Services at any time. Security-related events include, but are not limited to, the following:
 - User login success and failures
 - Failure to obtain privileged access
 - Access policy violations
- k. Computer naming must follow the Computer Naming Guidelines set forth by HCS. Computers not following the Computer Naming Guidelines may be renamed or removed from the network without notice.

All hardware and applications purchased by or for HCS is the sole property of HCS. All hardware, applications and and/or network infrastructure components that are issued to a user or location do not inherit any ownership rights from that user or location. Equipment or applications may be removed, installed, or upgraded as is required by Technology Services. HCS users shall not remove or move HCS issued hardware from room to room or school to school without approval from the Director of Technology Services.

V. Wireless Devices

- a. Sensitive applications shall not be hosted on wireless subnets or be transmitted over the wireless network without approval from Technology Services. No systems on wireless subnets should store or transmit data of a sensitive nature, such as credit card numbers, private student information, legal, or attorney privileged data.
- b. WAP security protocol will be mandatory on all wireless hardware, unless higher encryption or a more suitable protocol is available.
- c. All wireless hardware will be administered by Technology Services.
- d. Secondary wireless LAN connections are prohibited.

VI. Passwords

Employees need to be aware of their responsibility to keep their User ID and password(s) confidential. This section covers passwords and password procedures.

- a. School system passwords are considered confidential and shall not be released unless directed by the HCS, Superintendent, or the Director of Technology Services.
- b. School system passwords are initially assigned by Technology Services and shall be changed without notice as directed by the HCS, Superintendent, or the Director of Technology Services.
- c. The Superintendent, Director of Technology Services, Network Coordinator and appropriate Technology staff shall have access to and may change or modify passwords.
- d. Each user must have a unique user ID. As needed, administrators must be able to uniquely identify all users, including name, user identification and location.
- e. Users will not share their user ID and password. If Technology Services personnel must sign on to a user's account, and the password is not known, then the password will be reset to the system authorized password.
- f. .
- g. Maximum password age will be no older than forty-five days.
- h. Passwords should be memorized. User ID(s) or password(s) should be secured including those kept on mobile devices.
- i. Users should ensure that they are not being watched before entering a User ID or password. Users are responsible for making sure they avoid obvious "shoulder surfing" by students or other staff.
- j. Before using the User ID and password on a non-HCS computer, the user should make sure the computer is well protected, free of Malware or other software that might allow for a breach of security.

- k. Failed login sessions will be terminated and the account locked out after ten unsuccessful attempts. Account reinstatement is at the discretion of the HCS, Superintendent, or The Director of Technology Services.
- l. Minimum password length will be at least six characters, including special characters and numbers.
-
- m. Users will not be able to reuse the previous ten passwords.
- n. Users will not use special programs to login. Special programs include, but are not limited to, batch files, automatic log-in scripts, software macros, terminal function keys or other software.
-
- o. Vendor-supplied default passwords shall be changed before any computer, application or communications system is used.
- p. A password shall be changed if it is suspected of being disclosed to anyone besides the authorized user.
- q. Passwords are the property of the HCS and not the user.

VII. Anti-Virus and Anti-Malware Software

Malware is a very serious threat to critical school business data, network security and electronic infrastructure stability. As malware evolves, it will become more sophisticated, dangerous, and devastating. It is important that all network/computer users understand their role in preventing damage or loss of productivity based on malware threats.

- a. All desktops, servers, laptops, or at-risk operating systems will have the system default antivirus software installed and have current virus signatures.
- b. Users shall not download any files and/or programs from unknown sources.
- c. Users shall not open suspicious or non-job related attachments, even if they were sent by a friend, family member, or co-worker.
- d. Users shall scan make every effort to ensure that all externally connected devices are free of both viruses and malware.
- e.
- f. Users shall not download updates, Service Packs, or any software that might modify the current operating system or network environment.
- g. If a “stand-alone” (non-networked) machine is used, the machine must run the default HCS anti-virus software.
- h. Technology Services or software vendors do not e-mail updates, patches or complete software changes. If users receive suspicious e-mail directing as such the e-mail should be deleted.

VIII. Virtual Private Network (VPN)

This policy applies to all Henry County School employees, contractors, temporaries, and other workers including all personnel affiliated with third parties utilizing VPN's to access the HCS Network. Approved employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPN's, which are a “user managed” service. This means that the user is responsible for selecting an ISP, coordinating installation, installing any required software, trouble shooting as needed and paying associated fees.

- a. It is the responsibility of employees and vendors with VPN privileges to ensure that unauthorized users, i.e., family, coworkers and/or friends, are not allowed access to HCS internal networks.
- b. Vendors with authorized VPN access shall be asked to sign an acknowledgement of receipt of IFBGA policy.
- c. VPN connectivity shall be protected using password authentication.
- d. When actively connected to the corporate network, VPN's will force all traffic to and from the PC over the VPN tunnel; all other non-VPN traffic will be dropped.

- e. Dual (split) tunneling is not permitted; only one network connection is allowed.
- f. All computers connected to the HCS internal network via VPN or any other technology must use updated anti-virus software.
- g. VPN users will be automatically disconnected from the HCS network after thirty minutes of inactivity. The user must then reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
- h. Only HCS approved VPN client software may be used.
- i. By using VPN technology with personal home equipment, a user should understand that their machines are a de facto extension of the HCS network, and as such are subject to the same rules and regulations that apply to HCS owned equipment as related to school system job responsibilities.
- j. Any employee found to have violated this policy may be subject to disciplinary action, up to and including removal of VPN access, removal of HCS network access and possible termination of employment.

IX. Backup and Recovery

Operation guidelines as related to disaster recovery procedures are outlined in the HCS Disaster Recovery Plan. This section of the Network Security Policy addresses preservation of documents, e-mail storage and retention policies for network data.

- a. Stored tapes are centrally located in a fire safe within the HCS Data Center.
- b. Non-e-mail data is backed up daily. Data is retained for 10 days.
- c.
- d.
- e. E-mail (Exchange Information Store) data is backed up daily. E-mail data is kept for 14 days. Quarterly data backup is not available for e-mail data.
- f. Fund accounting backups are run on a bi-weekly, quarterly and a yearly rotation. Related data is stored within the fire safe at the HCS Data Center. Extended holiday periods that extend longer than a week are exempt from the bi-weekly schedule backup.
- g. Hardcopies of network and user passwords, AS400 passwords, and software administration passwords are stored in the fire safe at the HCS Data Center.
- h. Individual "mailbox" restores are not available for Exchange users.
- i. Open records requests are not possible 14 days after the user deletes the e-mail from their Exchange Mailbox.

X. PROHIBITED ACTIVITIES AND PENALTIES

The following are prohibited activities. Non-compliance shall result in disciplinary action being taken which can include termination of employment.

- a. General
 - i. Inappropriate or unauthorized communication.
 - ii. Printing or distributing copyrighted materials. This includes, but is not limited to, software, articles and graphics protected by copyright.
 - iii. Sending, printing, or otherwise disseminating HCS proprietary data or any other information deemed confidential by HCS, to unauthorized persons.

- iv. Operating a business, soliciting money for personal gain or otherwise engaging in commercial activity outside the scope of employment with Henry County Schools.
- v. Attempting to access non-job related websites to include, but not limited to pornography, online gaming, terrorism, espionage, theft, or drugs.
- b. E-mail
 - vi. Sending or forwarding messages for non-work related communication.
 - vii. Access to non-henry.k12.ga.us e-mail accounts.
 - viii. Non-HCS approved Instant Messaging (IM) software for use on HCS computer systems.
 - ix. Searching for employment outside Henry County Schools.
 - x. Making offensive or harassing statements based on race, color, religion, national origin, disability, age, sex, or sexual orientation.
 - xi. Sending or forwarding messages containing defamatory, obscene, offensive, or harassing statements. Employees should notify their supervisor and/or school administrator immediately upon receiving such a message.
 - xii. Sending or forwarding a message that discloses personal information without HCS authorization. This shall also include accessing, transmitting, receiving, or seeking confidential information about employees or students without authorization.
 - xiii. Sending ethnic, sexual-preference or gender-related slurs, and/or jokes via e-mail.
 - xiv. Sending or soliciting sexually oriented messages, text messages, videos or images.
 - xv. Transmission of information that is confidential under HCS policy, federal or state laws or regulations.
- c. Software
 - xvi. Downloading and loading software without the prior approval of HCS, or Director of Technology Services.
 - xvii. Using software that is not licensed by the manufacturer or approved by HCS.
 - xviii. Gambling or engaging in any other criminal activity in violation of local, state, or federal law.
 - xix. Engaging in unethical activities or content.
 - xx. Participating in activities, including the preparation or dissemination of content, which could damage HCS's image, reputation and/or financial stability
 - xxi. Accessing account of another employee without authorization from the HCS, Superintendent, or the Director of Technology Services.
 -
 - xiii. Using software from an unauthorized source, including, but not limited to, the Internet, home, friends, and/or colleagues.
 - xiv. Illegal reproduction of software.
 - xv. Software piracy
 - xvi. Unlawful use
- d. Network

- xxii. Permitting another person to use your designated username or password to access the network, Internet, student information system, or fund accounting system.
- xxiii. Each user's profile must not be readable, writeable, or executable by other users. Access to shared resources will be granted only as needed and must be authorized by the Director of Technology Services.
- xxiv. Guest network accounts.
- xxv. Impersonating another person while communicating or accessing the network or Internet.
- xxvi. Introducing malware, harmful component, corrupted data, or the malicious tampering with any of HCS's computer systems.
- xxvii. Remote administration, remote connection, terminal services, and Virtual Private Network (VPN) is prohibited for general users and may not be used, except by prior permission of HCS, Superintendent, or Director of Technology Services.
- xxviii. Access to another employee account unless authorized by the HCS, Superintendent, or Director of Technology Services.
- xxix. Any employee found to have violated this policy may be subject to disciplinary action, up to and including removal of VPN access, removal of HCS network access and possible termination of employment.
- e. HCS Policy federal and state laws or regulations
- xxx. Committing acts that violate HCS Policy, federal or state laws or regulations.

XI. COMPLIANCE

Each employee will be in compliance with HCS policies.

Any individual aware of a policy violation should immediately report the violation to their supervisor, School Administrator or the Director of Technology Services.

XII. NONCOMPLIANCE

Individuals who violate this policy and/or use HCS's e-mail system, network, software, or hardware access for improper purposes will be subject to disciplinary action, up to and including termination of employment.

HCS employees will be held responsible for attorney fees.

XIII. *Acceptable Use Policy*

Henry County Schools is pleased to bring Internet/World Wide Web access to school system staff and students (users). The purpose of this service is to provide teachers and students access to electronic resources that support job responsibilities and the teaching and learning process. Users access to the Internet and other computer resources is a privilege, not a right. Therefore, users who violate rules for the use of electronic resources shall be subject to revocation of these privileges and potential disciplinary and/or legal actions.

The Internet Safety Policy and school system measures are designed to address safety and security when using direct electronic communication. Electronic resources include but are not limited to Internet, World Wide Web (WWW), chat rooms, electronic mail, data, online resources, online services, portable media, network information, licensed software, telecommunication resources, HCS Intranet and all other school system electronic messaging systems and data systems. Communication over networks is not considered private. As needed, school officials can and will search data or e-mail stored on all school system-owned computers and networks.

All users are expected to comply with Board of Education policy IFBGA, Electronic Communications, and follow school system regulations for the use of electronic resources. Such regulations include but are not limited to the following:

1. Email accounts are provided for professional and academic purposes. Email accounts should not be used for personal gain, personal business activities or to solicit for non-school system business; broadcasting of unsolicited messages is prohibited
2. Use electronic resources to communicate confidential staff or student information only to those who are authorized to receive and with a need to know including student assessment data.
3. Follow school system regulations which concern the use of electronic resources (i.e., will not damage computers, will not violate the privacy of users' files, will follow directions of staff or supervisors, will not be wasteful of resources).
4. Comply with network policies (student and staff log-ins) including not circumventing desktop protection applications or internet filtering devices.
5. Use the Internet for appropriate educational resources.
6. Use electronic resources only with permission of an administrator or designated personnel.
7. Respect and comply with copyright laws (giving credit to the rightful author and not distributing protected materials or software) and do not download or transmit confidential or copyrighted information.
8. Immediately report security problems or policy violations to appropriate school and/or district staff.
9. Do not use electronic resources in a manner that is obscene, insulting, purposely inaccurate, intimidating or knowingly offensive to others.
10. Do not access inappropriate, obscene or vulgar materials or show others how to access or use them.
11. Do not transmit computer viruses or any other malicious programs.
12. Do not intentionally damage or disrupt Internet/WWW services or network/hardware/software that provides delivery of electronic resources.
13. Do not install or remove software on any computer or server.
14. Do not share user IDs or passwords.
15. Do not utilize unauthorized user IDs or passwords.
16. Do not post messages or information and attribute to another user.

School system staff will employ the same supervision and care in determining and monitoring appropriate use of the Internet. Short-term substitute teachers are not to take students to the computer lab nor allow students to use classroom computers. Long-term substitute teachers may be qualified to use computers / labs by building administration after they receive appropriate orientation including a review of the Authorized User Policy. Failure to abide by the Board policies and administrative procedures governing use of the school system's electronic resources may result in the suspension or revocation of system access, and can result in disciplinary action.

Henry County Schools has taken precautions, which are limited, to restrict access to inappropriate materials; however, on a global network it is impossible to control all available content. A user may accidentally or purposely discover inappropriate information. Use of any information obtained via electronic resources is at the risk of the user. Henry County Schools makes no warranties of any kind, whether expressed or implied, for the service it is providing. Henry County Schools will not be responsible for any damages a user may suffer, including loss of data or cost incurred from a commercial service. Henry County Schools will not be responsible for the accuracy or quality of information obtained through any telecommunication or electronic resource.

It is the policy of the Henry County Schools to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors, and (d) comply with the Children's Internet Protection Act [Pub. L No. 106-554 and 47 USC 254(h)].

XIV. DEFINITIONS

“Administrators” (Administration)

Central office administrators or school based administration

“HCS”

Henry County HCS of Education

Network

Includes any access to school system resources available from the school system network.

Instant Messaging (IM)

Any chat client that allows for instantaneous or near instantaneous messaging via the Internet or other LAN (Local Area Network) connections.

SIS

Malware, Viruses, SPAM or malicious code

A computer virus is a program written to alter the way a computer operates, without the permission or knowledge of the user. A virus must meet two criteria:

1. It must execute itself. It will often place its own code in the path of execution of another program.
2. It must replicate itself. For example, it may replace other executable files with a copy of the virus infected file. Viruses can infect desktop computers and network servers alike.

Anonymizers

An anonymizer or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable. It is a proxy server computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet. It accesses the Internet on the user's behalf, protecting personal information by hiding the client computer's identifying information

Henry County Schools

Date Adopted: 5/1/1996

Last Revised: 8/8/2005

Georgia Code	Description
O.C.G.A. 16-09-90	<u>Georgia Computer Systems Protection Act</u>
O.C.G.A. 16-09-91	<u>Computer Related Crime</u>
O.C.G.A. 16-09-92	<u>Definitions</u>
O.C.G.A. 16-09-93	<u>Computer crimes defined</u>
O.C.G.A. 16-09-93.1	<u>Misleading transmittal</u>
O.C.G.A. 16-09-94	<u>Violations</u>

These references are not intended to be part of the policy itself, nor do they indicate the basis or authority for the HCS to enact this policy. Instead, they are provided as additional resources for those interested in the subject matter of the policy.

Acceptable Use Policy

Henry County Schools is pleased to bring Internet/World Wide Web access to school system staff and students (users). The purpose of this service is to provide teachers and students access to electronic resources that support job responsibilities and the teaching and learning process. Users access to the Internet and other computer resources is a privilege, not a right. Therefore, users who violate rules for the use of electronic resources shall be subject to revocation of these privileges and potential disciplinary and/or legal actions.

The Internet Safety Policy and school system measures are designed to address safety and security when using direct electronic communication. Electronic resources include but are not limited to Internet, World Wide Web (WWW), chat rooms, electronic mail, data, online resources, online services, portable media, network information, licensed software, telecommunication resources, HCS Intranet and all other school system electronic messaging systems and data systems. Communication over networks is not considered private. As needed, school officials can and will search data or e-mail stored on all school system-owned computers and networks.

All users are expected to comply with Board of Education policy IFBGA, Electronic Communications, and follow school system regulations for the use of electronic resources. Such regulations include but are not limited to the following:

17. Email accounts are provided for professional and academic purposes. Email accounts should not be used for personal gain, personal business activities or to solicit for non-school system business; broadcasting of unsolicited messages is prohibited
18. Use electronic resources to communicate confidential staff or student information only to those who are authorized to receive and with a need to know including student assessment data.
19. Follow school system regulations which concern the use of electronic resources (i.e., will not damage computers, will not violate the privacy of users' files, will follow directions of staff or supervisors, will not be wasteful of resources).
20. Comply with network policies (student and staff log-ins) including not circumventing desktop protection applications or internet filtering devices.
21. Use the Internet for appropriate educational resources.

22. Use electronic resources only with permission of an administrator or designated personnel.
23. Respect and comply with copyright laws (giving credit to the rightful author and not distributing protected materials or software) and do not download or transmit confidential or copyrighted information.
24. Immediately report security problems or policy violations to appropriate school and/or district staff.
25. Do not use electronic resources in a manner that is obscene, insulting, purposely inaccurate, intimidating or knowingly offensive to others.
26. Do not access inappropriate, obscene or vulgar materials or show others how to access or use them.
27. Do not transmit computer viruses or any other malicious programs.
28. Do not intentionally damage or disrupt Internet/WWW services or network/hardware/software that provides delivery of electronic resources.
29. Do not install or remove software on any computer or server.
30. Do not share user IDs or passwords.
31. Do not utilize unauthorized user IDs or passwords.
32. Do not post messages or information and attribute to another user.

School system staff will employ the same supervision and care in determining and monitoring appropriate use of the Internet. Short-term substitute teachers are not to take students to the computer lab nor allow students to use classroom computers. Long-term substitute teachers may be qualified to use computers / labs by building administration after they receive appropriate orientation including a review of the Authorized User Policy. Failure to abide by the Board policies and administrative procedures governing use of the school system's electronic resources may result in the suspension or revocation of system access, and can result in disciplinary action.

Henry County Schools has taken precautions, which are limited, to restrict access to inappropriate materials; however, on a global network it is impossible to control all available content. A user may accidentally or purposely discover inappropriate information. Use of any information obtained via electronic resources is at the risk of the user. Henry County Schools makes no warranties of any kind, whether expressed or implied, for the service it is providing. Henry County Schools will not be responsible for any damages a user may suffer, including loss of data or cost incurred from a commercial service. Henry County Schools will not be responsible for the accuracy or quality of information obtained through any telecommunication or electronic resource.

It is the policy of the Henry County Schools to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors, and (d) comply with the Children's Internet Protection Act [Pub. L No. 106-554 and 47 USC 254(h)].