

ACCEPTABLE COMPUTER SYSTEM USE FOR STUDENTS AND GUESTS

This policy is approved by the Goochland County School Board and covers the usage of the school division's network and computer system. Its aim is to provide clear and fair guidelines for the use of the system which includes: the wireless (802.11) and wired data network available in each building across the division, desktop and laptop computers owned by the division, peripherals including but not limited to mice, keyboards, printers, digital cameras, scanners, video cameras, iPods, servers, and services provided across the network.

Introduction

This policy must be signed by guests who are granted access to the system, students over the age of 18, and parents of students younger than 18. The AUP will be kept on file by the school division for one year after it is signed. This policy must be signed before guests or students may use any portion of the computer system.

The computer system is configured and offered for educational uses and the professional business of the school division. Goochland County Public Schools administration may suspend or limit access to the division's computer system to any student or guest who violates this policy. The computer system is offered to help students and staff meet the mission and vision set forth by the school board for a quality educational experience. The system is shared by both employees and students. From time to time, we may have guests to the school division who require access to our system and/or network.

Connecting to our Network

This policy does not cover a student's or guest's ability to bring their own personal computing device to a school or school division building. Students may refer to their school's code of conduct for guidance on whether personal computing devices (computers, tablets, e-readers), MP3 players, and cell phones are permitted at your school.

A guest wireless network is provided at each school for visitors to use which is separate from the internal network at each school. This network provides filtered Internet access. Guests who bring their own laptops or computing devices must sign this document before being granted access to use our network. Students must secure approval from a building administrator to use their own personal computing device at school if it is banned through the student code of conduct at their school.

A password to access the Internet via the guest wireless network at each school is required via the school division's filter.

Compliance Statement

This AUP is in compliance with Virginia Department of Education requirements, and has been approved by the Goochland County School Board. This AUP is in compliance with National Telecommunication Rules and Regulations.

Copyright Statement

Content (documents, video, audio) produced by students and guests using the computer system owned by Goochland County Public Schools (GCPS) is the property of the individuals creating the content. Content produced by students, guests, or employees of GCPS published on Internet (web) servers operated by GCPS is the property of, and belongs to, Goochland County Public Schools.

Disclaimer

The school board is not responsible for any information that may be lost, damaged, or unavailable when using the computer system or for any information retrieved via the Internet. Furthermore, the school board will not be responsible for any unauthorized charges or fees resulting from access to the computer system.

The division superintendent shall submit to the Virginia Department of Education this policy and accompanying regulation biennially.

Acceptable Use

Each time students or guests use the computer system, they must abide by the policies outlined in this document.

Students and guests using the GCPS computer system will observe the privacy of others. Students will only use their own network credentials (login names and passwords) for access to the computer system.

Each student and guest will be provided a credential to be used to access services on the computer system. This credential is designed to be private and should not be shared with other students or guests. Students who learn of their credential becoming compromised should report the situation immediately to a staff member. Students are only permitted to access their network accounts themselves.

A student's credential may be used outside the system to access services over the Internet. Use of the division's own or contracted web services offsite falls under this acceptable use policy.

Behavioral standards using the computer system will follow the code of conduct for students. Students are encouraged to treat others "online" using the computer system with respect and courtesy.

Students and guests will have opportunities to use the computer system for communications, examples including synchronous voice and video chat, e-mail, blogging, document collaboration, and podcasting. Communication using the computer system must abide by a specific school assignment and the mission statement of the school. Communications outside the realm of assignments or approved school business are prohibited. School officials reserve the right to know with whom and about what students or guests are communicating as part of this policy's focus on student cyber safety.

The primary purpose of the computer system for students and guests is to conduct research, to share resources, and to create content for facilitating the learning process.

Acceptable Uses for Publishing Content

Students and guests may be provided resources for publishing original content on intranet (internal) and Web (public, external) servers. These resources may include tools and storage for publishing webpages, blogs, wikis, collaborative environments (GoogleApps) or an online course management system (examples: Blackboard, Moodle, etc.). With the public access to content made available on our computer system, students and guests must engage in responsible use of these resources. These resources are provided to promote communication and to serve as instructional tools used to enhance the learning process.

All publication of content by students to Web or Intranet servers will be supervised by teachers and staff members. Violations of this policy for use of the computer system or for publishing content online will result in revocation of publishing privileges. GCPS reserves the ownership rights of content published on its servers. GCPS will make a good-faith effort to educate and inform student publishers about legal issues surrounding copyright laws.

Language

Students will communicate and publish electronically in a way that demonstrates respect for others and one's self. Students or guests may not use obscene, profane, lewd, vulgar, rude, inflammatory, hateful, threatening, or disrespectful language using the computer system, including but not limited to, webpages, blogs, wikis, course management systems, instant messaging, GoogleApps, or electronic mail.

Information Quality

Students or guests may not knowingly or recklessly post false or defamatory information about a person or organization using the school division's computer system including but not limited to, webpages, blogs, wikis, course management systems, instant messaging, GoogleApps or electronic mail.

Non-Educational Use

Content published or communicated electronically from the division's computer system must be related to the educational mission prescribed by the school or classroom assignment. Students or guests may not use the school division's web servers to for personal use or to conduct business, or engage in communications outside the realm of a classroom project.

Unacceptable Uses

The following examples of behaviors with the computer system are prohibited. The division's Internet filter prevents many of these uses from taking place. However, the filtering appliance used by the division cannot prevent behaviors or rob users of the computer system of their responsibilities.

Bandwidth Hogging

The computer system is a shared resource. Students or guests may not download or stream large files over the network without an educational purpose and approval by a teacher or staff member. Examples of bandwidth hogging include: movie trailers, software applications, video streaming services (YouTube, etc.).

Vandalism

Any form of vandalism, including physical alteration or breakage of hardware, including cabling, keyboards, and mice, is prohibited. Altering or destroying files not owned by the individual is also vandalism. Examples include: writing on computers with markers, breaking a mouse, cutting network cables, deleting another student's documents, etc.

Stealing Credentials, Unauthorized Access

The stealing of credentials (login and password information) for staff, guests, or students is prohibited. Accessing the computer system with another student's or a staff member's credentials is prohibited.

Access of Content Owned by Others

Students may not have access to files and digital property created by staff on the computer system unless they are expressly being shared by the other party. Students may only access electronic documents when they are knowingly shared by others for collaborative projects and lessons.

Reconfiguration of network security measures, Bypassing Internet filtering

Students may not reconfigure the security measures in place by the school division to change access rights to computer files, or engage in activity that is considered "cracking", including: the use of proxy servers to bypass the Internet filter, changing the operating system permissions on files, attempting the use of "rootkits" to gain administrative access to the computer system, or changing the access rights assigned to students by the network administrator(s).

Use of external devices

Students may not use electronic devices not provided by the school division (including laptop computers, phones, or other "wi-fi" devices) on the school network without approval from school officials.

Games, Entertainment, and Social Networking

During the school day, students may not access online or locally-installed games or entertainment websites using the computer system. Likewise, access to social networking websites is prohibited.

Pornography

Students and guests may not use the computer system to access inappropriate content, including all forms of pornography.

Criminal Activity

Students and guests may not use the computer system to engage in any activity deemed illegal by local, state, or federal statutes, including the selling or purchase of illegal items or substances.

Malware & Software Installation

Students and guests are prohibited from installing, downloading, or distributing any software not owned by the school division, including "malware"—a class of software that includes viruses and trojan horses designed to interrupt or destroy services and data on the computer system.

Nuisance Behavior.

Students and guests are prohibited from using computer system resources to send chain letters, engage in "pyramid schemes", send unwanted e-mail (spam) or unwanted instant messages (spim).

Inappropriate Content

Unless approved for a research assignment, students and guests may not access content using the computer system that promotes or supports hate, bullying, violence, or discrimination.

Plagiarism

Students and guests may not use the computer system to commit plagiarism.

Cyber Safety

Goochland County Public Schools values the safety and security of each student. Since SY 2006-07, the school division has conducted training for each teacher on issues related to online safety in and outside of the division. In an effort to ensure the safety of students while using the computer system, the following policies focus upon cyber safety.

Monitoring

The school division will monitor the use of the computer system by guests and students. This includes observation by teachers and staff in the classroom and remote supervision across the network. Remote monitoring does not invoke the use of any cameras installed on computers at any time.

Internal Communication

Access to the Web makes communicating with anyone else on the Internet possible. Communication with any entity outside of the school division must be approved by building administration and without identifying students' full identity.

Instant Messaging

Access to online chat or instant messaging services will only be permitted when granted by a teacher or through a closed course management system operated by the school division.

Discussion Boards

Access to discussion boards will only be permitted when granted by a teacher or through a closed course management system operated by the school division.

Goochland County Public Schools will teach issues relating to cyber safety across the curriculum each school year. The school division may also elect to hold "information night" sessions for parents and the community relating to cyber safety and these sessions will be advertised on the school division's website.

Links to this AUP and the contents of a condensed version or an abbreviated summary of this policy will be posted as the "homepage" on each machine made available to students and guests. The following guidelines will likewise be posted with respect to cyber safety:

1. Do not share your identity, including your name, address, phone number, e-mail address, or where you attend school with anyone on the computer.
2. If you encounter any content online that makes you feel uncomfortable, share this content immediately with a teacher.
3. Only visit websites or use applications on the computer approved by your teacher.

Disclaimer. The School Board is not responsible for any information that may be lost, damaged, or unavailable when using the computer system or for any information retrieved via the Internet. Furthermore, the School Board will not be responsible for any unauthorized charges or fees resulting from access to the computer system.

The division superintendent shall submit to the Virginia Department of Education this policy and accompanying regulation biennially.

Student Name (printed): _____

Signature of Parent: _____

Date: _____

Before students or guests are permitted access to the computer system, the AUP from the Student Code of Conduct must be returned to the school, signed by the parent or guardian if the student is under the age of 18, or by the student, if age 18 or older.

ACCEPTABLE COMPUTER SYSTEM USE FOR STAFF

This policy is approved by the Goochland County School Board and covers the usage of the school division's network and computer system. Its aim is to provide clear and fair guidelines for the use of the system which includes: the wireless (802.11) and wired data network available in each building across the division, desktop and laptop computers owned by the division, peripherals including but not limited to mice, keyboards, printers, digital cameras, scanners, video cameras, iPods, servers, and services provided across the network.

Introduction

This policy must be signed by all staff who are issued network credentials, issued a laptop, or use any portion of the computer system as part of their job. The AUP will be kept on file by the school division for one year after it is signed. The agreement for this policy will normally be renewed at the time employment contracts are deployed.

The computer system is configured and offered for educational uses and the professional business of the school division. The computer system is offered to help students and staff meet the mission and vision set forth by the school board for a quality educational experience. The system is shared by both employees and students. From time to time, we may have guests to the school division who require access to our system and/or network.

Connecting to our Network

Staff may use the guest wireless network with their own personal computing devices (via wifi). Authentication using their provided account will be required to access the Internet. The school division offers no technical support in connecting to the wireless network with personal devices. The school division reserves the right to prevent a wifi device to connect to the wireless network if it is perceived to be a security risk or consumes unnecessary bandwidth. Employees should note that this network is not private and traffic across the network is monitored.

Compliance Statement

This AUP is in compliance with Virginia Department of Education requirements, and has been approved by the Goochland County School Board. This AUP is in compliance with National Telecommunication Rules and Regulations.

Copyright Statement

Content (documents, video, audio) produced by staff using the computer system owned by Goochland County Public Schools becomes the property of the school board. Content published on Internet (web) servers operated by GCPS is the property of, and belongs to Goochland County Public Schools.

Disclaimer

The school board is not responsible for any information that may be lost, damaged, or unavailable when using the computer system or for any information retrieved via the Internet. Furthermore, the school board will not be responsible for any unauthorized charges or fees resulting from access to the computer system.

The division superintendent shall submit to the Virginia Department of Education this policy and accompanying regulation biennially.

Acceptable Use

Each time a staff member uses the computer system, they must abide by the policies outlined in this document.

Staff using the Goochland County Public Schools computer system will observe the privacy of others. Staff will only use their own network credentials (login names and passwords) for access to the computer system, and these credentials may never be shared with students or guests.

Staff who learn of their credential becoming compromised should report the situation immediately to technology personnel.

A staff member's credential may be used outside the system to access services over the Internet. Use of the division's own or contracted web services offsite falls under this acceptable use policy.

Behavioral standards using the computer system for staff will follow the professional expectations for employees. This covers ethical use of the system and professionalism when using communications media (e-mail, blogs, instant messaging, websites, etc.).

The computer system may not be used for personal use during contract hours. Examples of personal use include but are not limited to: posting on Facebook, blogging about one's personal

life, consulting, running a business, selling merchandise, or soliciting other employees for business outside of school business.

Acceptable Uses for Publishing Content

Staff may be provided resources for publishing original content on intranet (internal) and Web (public, external) servers. These resources may include tools and storage for publishing webpages, blogs, wikis, collaborative environments (GoogleApps) or an online course management system (examples: Blackboard, Moodle, etc.). With the public access to content made available on our computer system, staff must engage in responsible use of these resources. These resources are provided to promote communication and to serve as instructional tools used to enhance the learning process.

Publication of content by staff to division Web or Intranet servers will be supervised by technology personnel. Violations of this policy for use of the computer system or for publishing content online will result in appropriate disciplinary action, based upon the circumstances. Goochland County Public Schools reserves the ownership rights of content published on its servers. Goochland County Public Schools will make a good-faith effort to educate and inform staff about issues surrounding copyright and the ethical publication of content.

Language

Staff will communicate and publish electronically in a way that demonstrates respect for others and one's self. Staff may not use obscene, profane, lewd, vulgar, rude, inflammatory, hateful, threatening, or disrespectful language using the computer system, including webpages, blogs, wikis, course management systems, instant messaging, GoogleApps, or electronic mail.

Information Quality

Staff may not knowingly or recklessly post false or defamatory information about a person or organization using the school division's computer system including, but not limited to, webpages, blogs, wikis, course management systems, instant messaging, GoogleApps or electronic mail.

Non-Educational Use

Content published or communicated electronically from the division's computer system must be related to the educational mission prescribed by the school or classroom assignment. Staff may not use the division's computer system for non-professional communications during contract hours (non-work related instant messaging, e-mail, blogging, status updates via social networks).

Unacceptable Uses

The following examples of behaviors with the computer system are prohibited.

Bandwidth Hogging

The computer system is a shared resource. Staff is asked to be mindful of the bandwidth impact of content they find online and discourage bandwidth hogging. Examples of bandwidth hogging might include: movie trailers, downloading software applications, video streaming services (YouTube, etc.).

Vandalism

Any form of vandalism, including physical alteration or breakage of hardware, including cabling, keyboards, and mice, is prohibited. Altering or destroying files not owned by the individual is also vandalism. Examples include: writing on computers with markers, breaking a mouse, cutting network cables, deleting another employee's or a student's documents, etc.

Stealing Credentials, Unauthorized Access

The stealing of credentials (login and password information) for staff, guests, or students is prohibited. Accessing the computer system with another student's or a staff member's credentials is prohibited.

Reconfiguration of network security measures, Bypassing Internet filtering

Staff may not reconfigure the security measures set in place by the school division to change access rights to computer files, or engage in activity that is considered "cracking", including: the use of proxy servers to bypass the Internet filter, changing the operating system permissions on files, attempting the use of "rootkits" to gain administrative access to the computer system, or changing the access rights assigned to staff by the network administrator(s).

Games, Entertainment, and Social Networking

During the school day, staff may not access online or locally-installed games or entertainment websites using the computer system. Likewise, staff may not access social networking websites during the school day not officially adopted by the school division. Examples include MySpace, Facebook, LinkedIn.

Pornography

Staff may not use the computer system to access inappropriate content, including all forms of pornography.

Criminal Activity

Staff may not use the computer system to engage in any activity deemed illegal by local, state, or federal statutes, including the selling or purchase of illegal items or substances.

Malware & Software Installation

Staff are prohibited from installing, downloading, or distributing any software not owned by the school division, including "malware"—a class of software that includes viruses and

trojan horses designed to interrupt or destroy services and data on the computer system. Exceptions include freeware or trials of shareware. Any software requiring purchase must be approved in advance by technology personnel.

Nuisance Behavior

Staff members are prohibited from using computer system resources to send chain letters, engage in "pyramid schemes", send unwanted e-mail (spam) or unwanted instant messages (spim).

Inappropriate Content

Unless approved for research, staff may not access content using the computer system that promotes or supports hate, bullying, violence, discrimination, or criminal activity.

Cyber Safety

Goochland County Public Schools values the safety and security of each student. Since SY 2006-07, the school division has conducted training for each teacher on issues related to online safety in and outside of the division. In an effort to ensure the safety of students while using the computer system, the following policies focus upon cyber safety.

Monitoring

The school division will monitor the use of the computer system by guests and students. Teachers will monitor student use of the computer system through classroom management. Technology staff may monitor student computers electronically. Remote monitoring does not invoke use of any cameras installed on computers.

Internal Communication

Access to the Web makes communicating with anyone else on the Internet possible. Classroom communication with any entity outside of the school division must be approved by building administration and without identifying the students' full identities.

Teaching CyberSafety

Teachers each year will be held responsible for teaching at least one division-approved lesson on one or more Internet Safety topics to students. In addition, the school division may also elect to hold "information night" sessions for parents and the community relating to cyber safety and these sessions will be advertised on the school division's website.

Disclaimer. The School Board is not responsible for any information that may be lost, damaged, or unavailable when using the computer system or for any information retrieved via the Internet. Furthermore, the School Board will not be responsible for any unauthorized charges or fees resulting from access to the computer system.

The division superintendent shall submit to the Virginia Department of Education this policy and accompanying regulation biennially.

Acceptable Use Agreement. As an employee of Goochland County Public Schools, I have read and understand the policy outlined above on Acceptable Use of the School Division's Computer System. I acknowledge failure to abide by this policy will result in action by the Superintendent outlined in the Employee Handbook.

This Acceptable Use Agreement expires on _____.

Employee Name (printed): _____

Employee Signature: _____

Date: _____

Adopted: August 10, 1999.

Revised: August 14, 2001.

Revised: October 9, 2001.

Revised: July 24, 2007.

Revised: July 13, 2010.

Legal Refs.: Code of Virginia, 1950, as amended §§ 18.2-372,
18.2-374.1:1, 18.2-390, 22.1-70.2 and 22.1-78

18 U.S.C. §§ 1460, 2256

47 U.S.C. § 254