

ACCEPTABLE COMPUTER SYSTEM USE FOR STUDENTS AND GUESTS

This policy relates to the use of the school division's computer system and network for students and guests who are granted access to our computers and/or network. Please refer to the separate policy for employees and staff. Within this policy, AUP refers to this document, and "computer system" refers to, but is not limited to, laptops, desktop computers, the computer network, and peripherals including mice, keyboards, printers, digital cameras, scanners, and video cameras. "GCPS" refers to the Goochland County Public School division.

Introduction. The AUP for Goochland County Public Schools (GCPS) is a guide for the safe, ethical, and responsible use of our computer system, which includes desktop and laptop-based computers, our network, with access to the Internet, and our servers for the storage of documents and services available both on our local-area network (LAN) and the Web. The GCPS school division believes that access to technology is paramount for being prepared for life in the twenty-first century. We are committed to educating each student with respect to twenty-first century skills in a safe and productive environment. 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.

This AUP was designed to establish clear and fair guidelines for the use of the computer system by students and guests (users) of the GCPS school division. Each user must abide by the guidelines set forth in this policy or forfeit their right to use this system. Violations of this policy may incur additional disciplinary action by the individual school, the division, and key violations will be reported to local, state, or federal authorities.

For students younger than 18 years of age, this AUP must be signed by a parent or legal guardian before access to the GCPS computer system is granted. For students older than 18 years of age, and guests of the school division, this policy must be signed by the user before access to the GCPS computer system is granted.

This AUP will be posted in computer labs and presented to guests visiting the schools who use our network or computer system.

Individual schools within GCPS must keep this signed document on file for each student for the duration of the school year.

File: IIBEA (Page 2)

The computer system is configured and offered for educational uses and the professional business of the school division. GCPS administration is guaranteed the privilege of suspending or limiting access to the division's computer system to any student or guest who violates this AUP. A "guest" is any person having permission to use the division's computer system who is not an employee or student.

Educational use and Advantages of the Computer System. GCPS makes available a variety of software applications for student use on its computer system, including browsers for interacting with websites, productivity software (word processing, spreadsheet, presentation), and space for the storage of user documents. The GCPS Computer System can be used for a variety of learning experiences and may provide advantages over other forms of learning. Examples of educational uses of the computer system include: the creation of documents in a variety of media (music, word processing, art), calculations and simulations, and interactive communication.

Backup of Data. While GCPS makes every effort to provide a reliable storage medium for student documents, GCPS advises all users to regularly back-up their documents to a portable storage medium, such as CD-R or a flash-based memory stick (USB Thumb Drive). The

responsibility for backup lies with users at their own cost.

Consequences of Violating this AUP. In compliance with the Children's Internet Protection Act (CIPA), access to content available on the Internet is filtered, which includes pornographic content, access to non-educational social spaces (MySpace, Facebook, Bebo, Twitter, etc.), private web-mail services, and other content considered objectionable by Goochland County Public Schools. Using proxy servers or other means to bypass this filtering mechanism is a violation of this policy.

All students and guests must abide by this policy for the use of the computer systems. Violations of this policy will result in disciplinary action by the school administration based on the severity of the infraction of policy. Refer to the Student Code of Conduct published by the Goochland County School Board for a discussion of violating this Acceptable Use Policy (AUP) and the Acceptable Use Agreement (AUG) signature page, required by a student's school, before use of the computer system will be permitted.

File: IIBEA (Page 3)

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 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.

Acceptable Use. Students may use their own photographs when publishing content to the Web if students are not identified, and if the directory information form (distributed in the Student Code of Conduct) has not been returned prohibiting the school division to publish the photographs of students.

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

Students and guests using the Goochland County Public Schools 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.

Behavioral standards using the computer system will follow the code of ethics 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, 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 students or guests are communicating as part of this policy's focus on student cyber safety.

File: IIBEA (Page 4)

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. The following examples outline unacceptable computer system use by students and guests.

Unacceptable Use

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. Examples include: writing on computers with markers, breaking a mouse, cutting network cables, etc.

Stealing Credentials, Unauthorized Access. The stealing of credentials (login and password information) for staff 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 read, delete, copy, or modify documents or files belonging to other users on the computer system, including other students and staff. 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. During the school day, students may not access online games or entertainment websites using the computer system.

File: IIBEA (Page 5)

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. Students and guests are prohibited from installing, downloading, or distributing "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.

Publishing Content Online. 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, 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 with one single purpose: to promote communication as part of the learning process.

All publication of content by students to Web or Intranet servers will be supervised by teachers and staff members. Violations of the policies listed above for acceptable and unacceptable use, and those below, for publishing content online, will result in revocation of publishing privileges. 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 student publishers about issues surrounding copyright and the ethical publication of content.

File: IIBEA (Page 6)

Acceptable and Unacceptable Use Policies for Publishing Content

Purpose. Students may be asked to publish content through webpages, blogs, wikis, a course management system, or other similar systems online using the World Wide Web or private web servers operated by the school division. These communication services are offered only as an instructional tool used to enhance the learning process.

Language. Students or guests 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, 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 webpages, blogs, wikis, course management systems, instant messaging, or electronic mail.

Non-educational use. Students or guests may not use the school division's web servers to conduct business, or engage in communications outside the realm of a classroom project.

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 and by the completion of SY 2007-08 will have integrated online safety into the core curriculum used by the school division in grades K-12. 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.

Internal Communication. Access to the Web makes communicating with anyone else on the Internet possible. Students may only communicate within the school division through the use of blogs, e-mail, or instant messaging. At times, a teacher may establish a project with students from another school division, or experts in their field of study. Communication with any entity outside of the school division must be approved by building administration and without identifying students' full identity.

File: IIBEA (Page 7)

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 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 in regards 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.

File: IIBEA (Page 8)

ACCEPTABLE COMPUTER SYSTEM USE FOR STAFF

This policy relates to the use of the division's computer system and network for employees who are granted access to our computers and/or network. Please refer to the separate policy for students and guests to the school division. Within this policy, AUP refers to this document, and "computer system" refers to, but is not limited to, laptops, desktop computers, the computer network, and peripherals including mice, keyboards, printers, digital cameras, scanners, and video cameras. "GCPS" refers to the Goochland County Public School division.

Introduction. The AUP for Goochland County Public Schools (GCPS) is a guide for the safe, ethical, and responsible use of our computer system, which includes desktop and laptop-based computers, our network, with access to the Internet, and our servers for the storage of documents and services available both on our local-area network (LAN) and the Web. The GCPS school division believes that access to technology is paramount for being prepared for life in the twenty-first century. We are committed to educating each student with respect to twenty-first century skills in a safe and productive environment. 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.

This AUP was designed to establish clear and fair guidelines for the use of the computer system by staff, teachers, and administrators (users) of the GCPS school division. Each employee must abide by the guidelines set forth in this policy to maintain the contractual obligations for employment. Violations of this policy can affect employment status at the individual school, in the division, and key violations will be reported to local, state, or federal authorities.

This policy must be signed by each employee of the school division as a condition of employment.

This AUP will be posted in computer labs and presented to guests visiting the schools who use our network or computer system.

The computer system is configured and offered for educational uses and the professional business of the school division. GCPS administration is guaranteed the privilege of suspending or limiting access to the division's computer system to any user who violates this AUP. A "guest" is any person having permission to use the division's computer system who is not an employee or student.

File: IIBEA (Page 9)

Educational use and Advantages of the Computer System. GCPS makes available a variety of software applications for employee use on its computer system, including browsers for interacting with websites, productivity software (word processing, spreadsheet, presentation), and space for the storage of user documents. The GCPS Computer System can be used for a variety of teaching and learning experiences and may provide advantages over other forms of learning. Examples of educational uses of the computer system include: the creation of documents in a variety of media (music, word processing, art), calculations and simulations, and interactive communication.

Teachers and administrators are encouraged to take advantage of staff development opportunities offered by the school division to increase comfort level with technology and to learn about pedagogical techniques using the computer system.

Backup of Data. While GCPS makes every effort to provide a reliable storage medium for user documents, GCPS advises all users to regularly back-up their documents to a portable storage medium, such as CD-R or a flash-based memory stick (USB Thumb Drive). The responsibility for backup lies with users at their own convenience. GCPS recommends employees back-up data on a weekly basis to a provided external hard disk drive.

Consequences of Violating this AUP. In compliance with the Children's Internet Protection Act (CIPA), access to content available on the Internet is filtered for students, which includes pornographic content, access to non-educational social spaces (MySpace, Facebook, Bebo, Twitter, etc.), private web-mail services, and other content considered objectionable by Goochland County Public Schools. Using proxy servers or other means to bypass this filtering mechanism is a violation of this policy. GCPS provides an override function for employees to gain access to blocked content on a "as-needed" basis solely for the purposes of conducting school business.

All employees must abide by this policy for the use of the computer systems. Violations of this policy will result in administrative action by the school administration based on the severity of the infraction of policy. Details regarding violation of this policy are outlined in the Employee Handbook published by the Superintendent of the school division.

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.

File: IIBEA (Page 10)

Copyright Statement: Content produced by employees of Goochland County on the computer system owned by the school division is property of GCPS. Content published by employees of GCPS on Internet (web) servers operated by GCPS is property of, and owned by GCPS. Employees may petition for copyright ownership for documents created using the computer system outside of contractual hours.

Acceptable Use: Each time employees use the computer system, they will abide by the policies outlined in this document.

Employees using the Goochland County Public Schools computer system will observe the privacy of others. Employees will only use their own account credentials (login names and passwords) for access to the computer system.

Each user 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 employees, students, or guests. Employees who learn of their credential becoming compromised should report the situation immediately to a technology staff member. Generic credentials--those intended for a large group to access content on the computer system--may be shared when using portions of the computer system with students.

Employees may be asked to help manage the credentials for student or guest use on the computer system. Employees privileged with this information must take care to maintain the confidentiality of student or guest credentials.

Employees who elect to share the use of their laptop computer with a family member are encouraged to create a separate account on the computer to protect the privacy of data under the employee's account. Employees who share their laptop with a family member take responsibility for compliance with this AUP.

Employees will have opportunities to use the computer system for communications, examples including synchronous voice and video chat, e-mail, blogging, and podcasting. Communication using the computer system must be consistent with each employee's assignment. Communications outside the realm of assignments or approved school business are prohibited. Employees must monitor student use of the computer system through a variety of means and report violations of the AUP for students and guests to school administrators.

File: IIBEA (Page 11)

Certified employees (teachers) will maintain a weblog (blog) provided by the school division for the purposes of communicating with community stakeholders, other teaching professionals, and students. Maintenance of the blog will follow the guidelines set forth, below, under "Publishing Content Online."

Employees issued an electronic mail account will regularly read and respond to mail messages. The account is used for official school business only, including communications between teaching colleagues, parents, and administration.

Teachers are required to regularly upkeep student grades and report attendance using our electronic grading and attendance system.

The primary purpose of the computer system for all users is to conduct research, to share resources, conduct school business and record keeping, and to create content for facilitating the learning process. The following examples outline unacceptable computer system use by employees.

Unacceptable Use 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. Examples include: writing on computers with markers, breaking a mouse, cutting network cables, etc.

Stealing Credentials, Unauthorized Access. The stealing of credentials (login and password information) for staff or students is prohibited. Accessing the computer system with another staff member's credentials is prohibited.

Access of content owned by others. Employees may not read, delete, copy, or modify documents or files belonging to other employees on the computer system. 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. Employees 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

File: IIBEA (Page 12)

"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. Employees 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 the division superintendent or his/her designee.

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

Criminal Activity. Employees 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. Employees are prohibited from installing, downloading, or distributing "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. Employees 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).

Publishing Content Online. Employees 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, or an online course management system (examples: Blackboard, Moodle, etc.). With the public access to content made available on our computer system, all users must engage in responsible use of these resources. These resources are provided with one single purpose: to promote communication as part of the learning process.

All teachers are required to maintain a weblog (blog). The blog will be updated with a new post at least once each week during the school year. 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 employee publishers about issues surrounding copyright and the ethical publication of content.

File: IIBEA (Page 13)

Teachers are encouraged to share the Web address (URL) of their blog with parents and students.

Acceptable and Unacceptable Use Policies for Publishing Content

Purpose. Employees may be asked to publish content through webpages, blogs, wikis, a course management system, electronic mail, or other similar systems online using the World Wide Web or private web servers operated by the school division. These communication services are offered only as an instructional tool used to enhance the learning process.

Language. Employees 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, or electronic mail.

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

Non-educational use. Employees may not use the school division's web servers to conduct business, or engage in communications outside the realm of their assignment.

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 and by the completion of SY 2007-08 will have integrated online safety into the core curriculum used by the school division in grades K-12. 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.

Internal Communication. Access to the Web makes communicating with anyone else on the Internet possible. Employees may only communicate within the school division through the use of blogs, e-mail, or instant messaging. At times, a teacher may establish a project with students from another school division, or experts in their field of study. Communication with any entity outside of the school division must be approved by building administration and without identifying students' full identity.

File: IIBEA (Page 14)

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.

Cyber Safety and Copyright and Ethics Training. Instructional employees new to Goochland County (administrators, teachers) must complete a staff development workshop on cyber-safety and copyright offered by the school division each school year. This workshop opportunity will be required of teachers seeking re-certification as part of the Technology Standards for Instructional Personnel (TSIP) requirement on a recommended basis by school division officials.

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: _____

File: IIBEA (Page 15)

Adopted: August 10, 1999.

Revised: August 14, 2001.

Revised: October 9, 2001.

Revised: July 24, 2007.

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

GOOCHLAND COUNTY PUBLIC SCHOOLS