GEORGIA CYBER ACADEMY ACCEPTABLE USE POLICY
The purpose of Georgia Cyber Academy's acceptable use policy is to provide the procedures, rules, guidelines, and code of conduct for using technology and the information network at Georgia Cyber Academy.

Definition

"Information Network" is any hardware and software configuration connecting users. The network includes all the computer hardware, operating system software, application software**,** and stored files. This includes but is not limited to electronic mail, local databases, externally accessed databases, recorded magnetic or optical media, clip art, digital images, digitized information, communications technologies, portable/hand-held devices, and new technologies as they become available. This acceptable use policy also governs standalone workstations. In addition to hardware and software, GCA protects students' personally identifiable information. The DOE defines Personal Identifiable Information (PII) as "Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means."

Further, PII is defined as information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Information permitting a specific individual's physical or online contact is the same as personally identifiable information. This information can be maintained in either paper, electronic or other media."

Introduction

Georgia Cyber Academy provides resources for teaching and learning, collaboration, communication services, and business data services by maintaining access to local, regional, national, and international sources of information.

Georgia Cyber Academy information resources will be used by staff and students following the policies and regulations established by Georgia Cyber Academy. These procedures do not attempt to articulate all required or prescribed behavior by its users.

Successful network operation requires the following:

1. All students conduct themselves in a responsible, decent, ethical, and polite manner while using the network.
2. The Student is ultimately responsible for their actions in accessing network services inside and outside of the Georgia Cyber Academy network while using Georgia Cyber Academy loaner equipment.
3. The Student is solely responsible for all resources issued or assigned to them. This includes equipment as well as login/specialized access information. In addition, any personal equipment used to access the Internet or other Georgia Cyber Academy resources is subject to the same rules and regulations outlined in this policy.
4. Georgia Cyber Academy monitors all Internet and local network activity.
5. Disciplinary action will be taken for anyone abusing or misusing technology resources.

Disclaimer

Access to computers and people worldwide also comes with the availability of materials that may not be considered educational value in the school setting. On a global network, it is impossible to control all materials, and a diligent user may discover controversial information. Georgia Cyber Academy maintains and monitors the use of filters for Internet content. Georgia Cyber Academy firmly believes that the valuable information and interaction available on this worldwide network far outweigh the possibility that users may obtain materials inconsistent with the educational goals of Georgia Cyber Academy.

Guidelines

1. Access to the networks and the information technology environment within Georgia Cyber Academy is a privilege and must be treated as such by all users of the network and its associated systems.
2. Georgia Cyber Academy systems will be used for research, education, and school-related business and operations.
3. Any system which requires password access or for which Georgia Cyber Academy requires an account may only be used by the authorized user. Account owners are ultimately responsible for all activity under their accounts.
4. All communications and information accessible via Georgia Cyber Academy systems should be treated as the property of Georgia Cyber Academy.
5. Georgia Cyber Academy monitors all Internet and local network activity, including individual actions and activity.

Unacceptable Uses

Georgia Cyber Academy has the right to take disciplinary action, remove computer and networking privileges, and/or take legal action for any activity characterized as unethical and unacceptable. Unacceptable use activities constitute, but are not limited to, any activity through which any user does the following:

1. Violates such matters as institutional or third-party copyright, license agreements, or other contracts. The unauthorized use of and/or copying of software is illegal.
2. Copies or reproduces any licensed software on Georgia Cyber Academy computing equipment, except as expressly permitted by the specific software license. Unauthorized use of the software is regarded as a serious matter, and any such use is without the consent of Georgia Cyber Academy.
3. Installs unauthorized software or applications on Georgia Cyber Academy computers.
4. Interferes with or disrupts other network users, services, or equipment. Disruptions include, but are not limited to, the distribution of unsolicited advertising.
    i. Propagation of computer worms or viruses.
    ii. Distribution of quantities of information that overwhelm the system (for example, "chain letters," "network games," or "broadcasting" messages).
    iii. Utilization of the network to make unauthorized entry into any resources accessible via the network.
5. Seeks to gain or gain unauthorized access to information resources, obtains copies of, modifies files or other data, or gains and communicates passwords belonging to other users.
6. Uses or knowingly allows another to use any computer, computer network, computer system, program, or software to devise or execute a scheme to defraud or to obtain money, property, services, or other things of value by pretenses, promises, or representations.

7. Destroys, alters, dismantles, disfigures, prevents rightful access to, or otherwise interferes with the integrity of computer-based information, its operation, and/or information resources, whether on stand-alone or networked computers.
8. Invades the privacy of individuals or entities.
9. Uses the network for commercial or political activity.
10. Uses the network to store, distribute, or access materials inappropriate to the Georgia Cyber Academy setting.
11. Uses Georgia Cyber Academy systems to compromise its integrity ("hacking" software).
12. Submits, publishes, or displays defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented, or threatening materials or public or private messages.
13. Uses Georgia Cyber Academy systems for illegal, harassing, vandalizing, inappropriate or obscene purposes or in support of such activities. Illegal activities will be defined as violating local, state, and/or federal laws. Harassment is defined as slurs, comments, jokes, innuendoes, unwelcome compliments, cartoons, pranks, and/or other verbal conduct relating to an individual with the following purposes or effects.
    i. Creating an intimidating, hostile, or offensive environment.
    ii. Unreasonably interfering with an individual's work or school performance.
    iii. Interfering with school operations.
14. Vandalism is any attempt to temporarily or permanently harm or destroy an operating system, application software, data, or hardware.

Georgia Cyber Academy Rights
Georgia Cyber Academy reserves the right to do the following:
1. Monitor all activities on Georgia Cyber Academy equipment and networks by any user
2. Determine whether specific network uses are consistent with this acceptable use policy.
3. Log network use and monitor storage disk space utilization by users.
4. Deem what is appropriate use based on the requirements of the law, this policy, and Georgia Cyber Academy's legitimate pedagogical concerns.
5. Remove a user's access to the network at any time it is determined that the user is engaged in unauthorized activity or violating this acceptable use policy and suspend any accounts during an investigation of possible violations of this policy.
6. Cooperate fully with any investigation concerning or relating to Georgia Cyber Academy.

Georgia Cyber Academy Responsibilities
Georgia Cyber Academy will do the following:
1. Respect and enforce copyright laws and regulations.
2. Take prudent steps to develop, implement and maintain security procedures to ensure the integrity of the individual and Georgia Cyber Academy files. However, information on any computer system cannot be guaranteed to be inaccessible by other users.
3. Attempt to provide error-free and dependable access to technology resources associated with Georgia Cyber Academy. However, Georgia Cyber Academy cannot be held liable for any information lost, damaged, or unavailable due to technical or other difficulties.
4. Thoroughly investigate alleged misuse of the Internet and/or Georgia Cyber Academy before the permanent denial of access to Georgia Cyber Academy resources.
5. Conduct assessments of inappropriate sites.
6. Monitor student Internet activities to ensure students and employees are not accessing inappropriate sites. The school Georgia Cyber Academy will use technology protection measures

to protect students and employees from improper access.

7. Expect all students using Georgia Cyber Academy resources will be monitored by an adult(s).
8. Report child pornography to law enforcement. Georgia Cyber Academy and school technical support staff working with any computer or portable device and coming across sexually explicit images of children must report this to local law enforcement. The report must include the name and address of the computer's owner or person.

Disciplinary Action
This acceptable use policy applies to any Georgia Cyber Academy community member and refers to all information resources, whether individually controlled, shared, stand-alone, or networked. Disciplinary action, if any, for students, staff, and other users will be consistent with Georgia Cyber Academy's standard policies and practices.

Where external networks are used, policies governing such use are also applicable and must be adhered to. Violations can cause revocation of access privileges, suspension, or permanent removal of access to Georgia Cyber Academy resources, another school disciplinary action, and/or appropriate legal action. Exact disciplinary measures will be determined on a case-by-case basis.

Any user who violates the terms of this policy or otherwise misuses the Internet and/or technology to access or send inappropriate material will be subject to disciplinary action up to and including for students: removal of access, suspension, or withdrawal.

Violations of the laws of the United States or the state of Georgia also may subject the user to criminal prosecution.

Code of Conduct
Proper behavior, as it relates to the use of technology, is no different than appropriate behavior in all other aspects of Georgia Cyber Academy activities. All users must use Georgia Cyber Academy technology resources legally, responsibly, ethically, and politely. A student who knowingly violates any portion of the Code of Conduct Expectations will be subject to suspension of access and/or revocation of privileges on the Georgia Cyber Academy's system and will be subject to disciplinary action under the Georgia Cyber Academy District Student and Parent Handbook.

1. Students will practice responsible use of digital information regarding intellectual property, including complying with software licenses, copyright laws, and all other state and federal laws governing intellectual property. Students will practice safe and appropriate online behavior, including professional etiquette. Improper use of Georgia Cyber Academy technology resources is prohibited, including but not limited to the following:
   i. Using racist, profane, pornographic, sexually-oriented, or obscene language or materials.
   ii. Attempting to send or sending anonymous messages of any kind.
   iii. Using the network to access inappropriate and/or harmful materials.
   iv. Bypassing Georgia Cyber Academy's security measures to access sites filtered on the Georgia Cyber Academy network.
   v. Encrypting communications to avoid security review or monitoring by the system administrator.
   vi. Misusing the network to provide addresses or other personal information that others may use.
   vii. Purposely engaging in activity that may harass, threaten, defame, slander, libel, malign, or

        abuse another (i.e., individual or group).

    viii. Forgery or attempted forgery of electronic messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users or deliberately interfere with the ability of other system users to send/receive electronic mail is prohibited.

    ix. Using the network for illegal purposes, in support of illegal activities, or for any other activity prohibited by Georgia Cyber Academy policy or guidelines.

    x. Communicating with other students outside of class using platforms such as, but not limited to, Google Docs, Google Slides, social media, and online communication forums.

2. Students will use the technology resources positively and responsibly, promoting creativity & innovation, collaboration, communication, critical thinking & problem-solving. Improper use of Georgia Cyber Academy's technology resources is prohibited, including but not limited to the following:

    i. Using the network for political activity, financial gain, or commercial activity.

    ii. Attempting to harm or harming equipment, materials, or data.

    iii. Changing any computer configurations and/or settings.

    iv. Installing software, including freeware and file-sharing services.

    v. Deliberate attempts to degrade or disrupt system performance may be viewed as violating Georgia Cyber Academy guidelines and, possibly, as criminal activity under applicable state and federal laws. This includes, but is not limited to, the uploading or creating of computer viruses, malware, or spyware.

    vi. Streaming media, such as radio, games, video, etc., for non-educational purposes

    vii. Proxy sites - Attempting to bypass, or bypassing, the filtering device by using sites such as but not limited to proxy sites on Georgia Cyber Academy's electronic communications system. Examples include but are not limited to chat rooms and video conferencing tools.

    viii. Running security programs or utilities that reveal or exploit weaknesses in the security of a system, such as a password cracking programs, packet sniffers, port scanners, or any other non-approved programs on Georgia Cyber Academy technology resources.

3. Students will understand the negative impact of inappropriate technology use, including online bullying and harassment, hacking, intentional virus setting, invasion of privacy, and piracy of software, music, video, and other media.

4. Students will log in to the Georgia Cyber Academy network using their login credentials. Account information and passwords, or similar information used for identification and authorization, must be kept private. Passwords should not be written down and left in a location where others may find them. The individual in whose name a system account is issued will always be responsible for its proper use.

5. To help preserve both privacy and security, neither still photography nor video capturing is allowed in person nor virtual school environments unless directed by a member of a faculty member to meet an educational goal or approved by an authorized member of the administration, faculty, or staff. Both behavioral and legal action may be taken against individuals not respecting these privacy and security rights.

6. Students will use technology resources cautiously to maintain security and prevent damage.

7. Students are asked to conserve Georgia Cyber Academy technology resources (such as network bandwidth and storage) by limiting usage to educational purposes. System users must not: degrade the performance of Georgia Cyber Academy technology resources (i.e., streaming video, streaming audio, and Internet radio); deprive an authorized Georgia Cyber Academy user access

to a Georgia Cyber Academy resource, obtain extra resources beyond those allocated; circumvent Georgia Cyber Academy computer security measures.

8. Creative Credit and Copyright. Students have the right to protect their creative works. Students must exercise academic integrity. Failure to cite ideas or work independently will result in adverse academic and behavioral action. Academic Integrity protects against the following:

   i. ***Cheating*** is fabricating written assignments; giving or receiving aid to another student without the consent of the instructor on tests, quizzes, assignments, or exams; unauthorized access to teacher's editions or answer keys. Cheating also includes using technology such as computers, phones, cameras, or any other device that provides access to unauthorized information related to graded course material, tests, quizzes, assignments, or examinations.

   ii. ***Double Assignments*** are also a form of cheating. This assignment is used to fulfill the requirements of more than one course without prior approval from all involved instructors.

   iii. ***Colluding*** allows one's work to be copied or submitted by another student. This applies to individual and group work, where the students are given individual grades. It also applies to work transferred electronically and submitted by another student. Joint student projects where information is combined for a final product submission are acceptable.

   iv. ***Plagiarizing*** is the act of presenting the ideas or works of another person as one's own. This includes giving information, ideas, phrasing, words, artwork, music, figures, diagrams, graphs, song lyrics, films, maps, illustrations, data, computer programs, emails, CDs, and electronic files from the Internet. This also includes the use of Artificial Intelligence (AI) tools to generate products and submit them for a graded assignment. All graded written assignments must include properly cited resources. Consult your instructor or the school links for appropriate citation practices. All assignments submitted to instructors should contain the correct citation. Plagiarism occurs when a student does one of the following: 1) fails to cite borrowed, quoted, or paraphrased material, even by accident; 2) deliberately intends to deceive through lack of citation; 3) uses strings of words from a cited source without indicating these words are not his own (attempted paraphrase without quotations, even if there is a correct citation).

      1. Carelessly or inaccurately citing quoted or paraphrased material is not plagiarism. This type of error is attributed to style or formatting. For example, if you submit an ALA works cited instead of an APA, then this is an inaccurate citation. You may lose style or formatting points; however, it is not plagiarism.

Digital Rights

At Georgia Cyber Academy (Georgia Cyber Academy), we work hard to ensure the following digital rights for all students.

1. Each student shall have access to current, updated, and fully functioning technologies to be used in the learning process.
2. Each student shall be given access to their Georgia Cyber Academy (Georgia Cyber Academy) username and password.
3. Each student shall be taught to access resources such as Gmail and Google Drive and learning management system (LMS) accounts connected to their Georgia Cyber Academy account.
4. Each student shall be allowed to attend classes led by teachers who blend technology into learning and assessment activities.
5. Each student shall be offered ongoing workshops and educational opportunities to better blend technology into the learning process.

6. Each student can use online collaborative tools in the learning process.
7. Each student shall enjoy an educational experience free from cyberbullying, harassment, or threats.

Loaner Equipment Issuing and Returns
Equipment Request
The enrolling legal guardian can request one (1) loaner student Chromebook for each enrolled student and one (1) loaner student printer for their household. The legal guardian may contact their assigned FEL to change an equipment request on the enrollment application.

Equipment Troubleshooting and Replacements
All technical issues with GCA-provided equipment must be reported to SCA Support by email at support@sca-atl.com or by phone at 404-334-4790 ext.8. If a replacement is deemed necessary during troubleshooting with an SCA Solutions Engineer, a replacement device will be shipped to the primary address on file with GCA. Please return prior defective devices, equipment assigned to withdrawn students, and/or curriculum-based equipment from a prior school year to ensure the shipment of the replacement device is completed on time.

Equipment Returns
When an equipment shipment is received, please keep all boxes for future returns. Returns can be completed by emailing the GCA Equipment Team at gcaequipment@georgiacyber.org to request a prepaid UPS return shipping label or a courier pickup. All courier pickups (within Georgia) are subject to approval. Your courier request must include the correct pickup address and best contact phone number. To avoid invoicing, all equipment is expected to be returned within two weeks of the delivery date of the new equipment. Failure to return your equipment during that time will result in invoicing with the potential to be deferred for collections. All devices must be returned or paid for in full. If outstanding equipment is sent to collections, families will be responsible for the cost of the equipment, plus the 24% collections fee.

Loaner Chromebook Program Responsibilities and Expectations
Students:
1. Are required to abide by the Acceptable Use Policy.
2. Will receive a Chromebook, when requested, as an educational tool, and it should only be used in that capacity. They are responsible for the care of the Chromebook issued to them, whether in or out of school.
3. Ensure the Chromebook is charged and ready for use every day.
4. Have a power cord and Chromebook bag and carry the Chromebook in the school-issued bag. If the power cord or bag is lost, damaged, or stolen, the student will pay for a new one.
5. Will lose Chromebook privileges if the student is responsible for any vandalism, hacking, network disruption, or any actions that disable, damage, or negatively affect the Chromebook or any GCA systems in any way.
6. Will only use software permitted and installed by the school Georgia Cyber Academy.
7. Acknowledge there is no expectation of privacy with files stored on the computers or with websites visited with the Chromebook. The school Georgia Cyber Academy has the right to monitor Chromebooks and/or block access to applications and websites.
8. Will NOT loan/borrow Chromebook, power cord, or bag to/from other students and will NOT share usernames and passwords.
9. Will NOT deface Chromebook by marking or placing stickers on all surfaces.

10. Will report damages **immediately** to Southeastern Computer Associates Support.
11. Will return the Chromebook, printer, hotspot (if applicable), Zoomy (if applicable), bag, and power cord if a student fails to show up after enrollment, graduates, transfers, and/or is withdrawn from the school. If needed, a return label and box will be provided, so our families incur no additional expense. All school equipment must be returned in good condition within two weeks of graduation or withdrawal.
12. Please return school property upon request to avoid families being invoiced. Unpaid invoices will result in GCA contacting collections agencies and/or filing police reports. If deferred to collections, a fee of up to 24% may be assessed due to failure to return loaner equipment at the time due.

Loaner Chromebook Program Warranty and Damage Protection Information

Warranty Information,
The manufacturer's warranty covers all Chromebooks for malfunction due to manufacturing or non-performance issues. The warranty does not cover damage determined to be accidental and/or the result of negligent use or treatment. It also does not cover outright loss or damage of the Chromebook, power cord, or batteries through inattention or negligence.

Negligence
Warranty coverage and damage insurance do not cover damages caused by negligent use/treatment, nor do they protect the power cord, battery, or laptop bag. **When the administration determines that negligent actions caused damage, the student or parent/guardian will be responsible for all costs.** Negligence is defined as the lack of care for the device that results in damage. For example, dropping the device would be considered an accident, whereas leaving the device in your car is negligence. A temporary computer will be provided when a deposit, not to exceed the cost of the device, is received from the Legal Guardian or Parent.

Reporting Procedure
Damage must be reported immediately to Southeastern Computer Associates Support. If the damage is determined to be accidental, a damage claim will be processed, and an invoice will be sent to the parents. A replacement Chromebook will be provided. A police report must be filed to process a theft claim.

STUDENT INTERNET USE AGREEMENT

_____   _____
  Student Name (Last, Middle Initial, First)   Grade

I have read and understood the rules and requirements for online access. I agree to abide by the rules, and I further understand that any violation of the regulations is unethical and may constitute a criminal offense. I understand that Georgia Cyber Academy is monitoring all of my activity on the Internet while using my GCA device. I understand that I am responsible for returning all equipment, including a printer, bag, and power cord. Should I commit any violation, my access privileges may be revoked for the remainder of the year. School disciplinary and/or legal action may be taken.

_____   _____
  Student Signature   Date

PARENT / GUARDIAN AGREEMENT

As the parent/guardian of this student, I have read the Georgia Cyber Academy Acceptable Use Policy. I understand that this access is designed for educational purposes. I recognize Georgia Cyber Academy can't restrict access to all controversial materials, and I will not hold them responsible for materials acquired on the network.

In compliance with the Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505 (COPPA), GCA must advise parents that we create accounts required for educational purposes that may or may not use the personal data of children, such as names, birthdays, grades, and GCA Email addresses. GCA requires the parent or legal guardian's consent to create educational accounts for the student(s) to receive a complete education from GCA in our online learning environment. Your signature below provides consent for GCA to create accounts through internal and 3rd party educational platforms.

I can be contacted at the phone number below to verify my permission. If I have questions regarding topics my child is researching or how my child is using the Internet, I will contact their teacher. I understand that Georgia Cyber Academy is monitoring all of my child's activity on the Internet while using Georgia Cyber Academy. I hereby permit my child to access information on the Internet.

I understand that I am responsible for returning all GCA-provided equipment promptly. I am responsible for the cost of any unreturned equipment.

_____   _____
Parent/Guardian Name (Last, Middle Initial, First)   Phone Number

_____   _____
Parent/Guardian Signature   Date