CALHOUN COUNTY
SCHOOL DISTRICT
FOCUSED ON SUCCESS FOR ALL!

Acceptable Use Policy and Email Guidelines

Introduction

Calhoun County Board of Education (—the Board) recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21st-century technology and communication skills. To that end, we provide access to technologies for student and staff use. This Acceptable Use Policy outlines the guidelines and behaviors that users are expected to follow when using school technologies or when using personally-owned devices on the school campus or in connection with school activities. Each user will be provided access to this policy and will sign an agreement to abide by its terms before establishing an account.

- The school board‘s network is intended for educational purposes.
- All activity over the network or when using district technologies may be monitored and retained. Access to online content via the network may be restricted in accordance with our policies and federal regulations, such as the Children‘s Internet Protection Act (CIPA).
- Students are expected to follow the same rules for good behavior and respectful conduct online as offline.
- The Board‘s policies, regulations, and rules of conduct apply not only to the use of school-owned resources but also to personally-owned technology resources brought on school property or used in connection with school activities.
- The Board‘s disciplinary jurisdiction may include off-campus activity that threatens the school‘s ability to maintain a safe and orderly environment (Board Disciplinary Jurisdiction, 5.16 in Policy Manual and page 3 in Student Handbook).
- Misuse of school resources or personal devices can result in disciplinary action. Users may be financially liable for damage/loss from misuse or negligence.
- The Board makes a reasonable effort to ensure students‘ safety and security online, but will not be held accountable for any harm or damages that result from the use of school technologies.

- Users of the district network or other technologies are expected to alert the Technology Department or local administrative staff immediately of any concerns for safety or security.

Technologies Covered

The Board may provide Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more. As new technologies emerge, The Board will attempt to provide access to them. The policies outlined in this document are intended to cover all available technologies, not just those specifically listed. This includes personally-owned devices, such as cell phones or other mobile devices, when used on the school campus or in connection with school activities.

Usage Policies

All technologies provided by the district are intended for education purposes. All users are expected to use good judgment and to follow the specifics of this document as well as the spirit of it: be safe, appropriate, careful, and kind; do not try to get around technological protection measures; use good common sense, and ask if you don‘t know.

Web Access

The Board provides its users with access to the Internet, including websites, resources, content, and online tools. That access will be restricted in compliance with CIPA regulations and school policies. Web browsing may be monitored and web activity records may be retained indefinitely. Users are expected to respect that the web filter is a safety precaution, and should not try to circumvent it when browsing the Web. If a site is blocked and a user believes it shouldn‘t be, the user should follow district protocol to alert a technology staff member or submit the site for review.

Email

The Board may provide users with email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies.
If users are provided with email accounts, they should be used with care. Users should not send personal information; should not attempt to open files or follow links from an unknown or questionable origin; should use appropriate language, and should only communicate with other people as allowed by the district policy. Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived.

Social / Web 2.0 / Collaborative Content

Recognizing the benefits collaboration brings to education, The Board may provide users with access to websites or tools that allow communication, collaboration, sharing, and messaging among users. Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally-identifying information online.

Mobile Devices

The Board may provide users with mobile computers or other devices to promote learning outside of the classroom. Users should abide by the same acceptable use policies when using school devices off the school network as on the school network.

Users are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to your care. Users should report any loss, damage, or malfunction to the Technology Department or local administrative staff immediately. Users may be financially accountable for any damage or loss resulting from negligence or misuse. Use of school-issued mobile devices off the school network may be monitored.

Personally-Owned Devices

Users should keep personally-owned devices (including laptops, tablets, smartphones, and cell phones) turned off and put away during school hours except as authorized or directed by school personnel.

In all matters involving the use or possession of personally-owned devices, students are expected to abide by the Code of Student Conduct, the Cell Phone Policy, and all other applicable school policies and rules.

Because of security concerns, when personally-owned mobile devices are used on campus, they should not be used over the school network without express permission from Technology staff.

Security

Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or questionable origin.

If you believe a computer or mobile device you are using might be infected with a virus, please alert the Technology Department. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

Downloads

Users should not download or attempt to download or run programs over the school network or onto school resources without express permission from school personnel. For the security of our network, users should download only authorized files from reputable sites, and only for educational purposes.

Netiquette

Users should always use the Internet, network resources, and online sites in a courteous and respectful manner. Users should also recognize that among the valuable content online there is unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the Internet. Users should also remember not to post anything online that they would not want parents, teachers, or future colleges or employers to see. Once

something is online, it‘s out there—and can sometimes be shared and spread in ways you never intended.

Plagiarism

Users should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet. Users should not take credit for things they didn‘t create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

Personal Safety

Users should never share personal information, including phone number, address, social security number, birth date, or financial information, over the Internet without adult permission. Users should recognize that communicating over the Internet or other electronic means brings certain risks, and should carefully safeguard personal information. Users should never agree to meet with someone that they met online —in real lifell without parental permission. If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult. Students should immediately bring any threatening or unwelcome communications to the attention of school personnel.

Cyberbullying

Cyberbullying will not be tolerated. Harassing, threatening, insulting, impersonating, excluding, and cyberstalking are all examples of cyberbullying. Do not send or post electronic communications with the intent of scaring, hurting, or intimidating someone else. Engaging in these behaviors or any online activities intended to physically or emotionally harm another person will result in serious disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Remember that your activities are monitored and retained.

Access and Privacy

All users will be provided with network storage space and should use only those accounts, files, software, and technology resources that are assigned to him/her. Network storage areas will be treated like school lockers. Network administrators will review files and communications to maintain system integrity and ensure that users are using the system responsibly. Users of school technology resources have no personal right of privacy or confidentiality with respect to the use of such resources and should not expect files, information, or communication stored on school resources to be private.

Unauthorized Access

Individuals shall not attempt to log in to the network by using another user's account and/or password or allow someone to use his/her password to access the network, email, or the Internet. Individuals must not attempt to modify technology resources, utilities, and

configurations, or change the restrictions associated with his/her accounts, or attempt to breach any technology resources security system, either with or without malicious intent. Individuals must not attempt to disrupt any computer services or data by spreading viruses, spamming, hacking, or any other means.

Data Integrity

Individuals shall not attempt to make fraudulent charges or modify data maliciously. Individuals shall not trespass or make changes in another user's work, folders, or files.

Inappropriate Materials or Language

No profane, obscene, lewd, inflammatory, abusive, harassing, threatening, discriminatory, or impolite language should be used, nor should materials be accessed which are not in line with the rules of school behavior. Materials placed on or linked to the system or school-sponsored Web pages must be preapproved by an administrator or authorized designee. Sending or displaying offensive, obscene, or sexually explicit messages or pictures is not permitted.

Examples of Acceptable Use:

Users will:

- Use school technologies for school-related activities.
- Follow the same guidelines for respectful, responsible behavior online that students are expected to follow offline.
- Treat school resources carefully and alert staff if there is any problem with the operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert a teacher or other staff member of threatening, inappropriate, or harmful content (images, messages, posts) online.
- Use technologies at appropriate times, in approved places, for educational pursuits. Cite sources when using online sites and resources for research.
- Recognize that use of school technologies is a privilege and treat it as such. Be cautious to protect the safety of self and others.
- Help to protect the security of school resources.

*This is not intended to be an exhaustive list.

Examples of Unacceptable Use:

Users will not:

- Use technologies to hurt, harass, attack or harm other people or their work.
- Attempt to find or access inappropriate websites, images, or content.
- Use language online that would be unacceptable in the classroom.
- Engage in cyberbullying, harassment, or disrespectful conduct toward others

- Damage computers, computer systems, or computer networks in any way (this includes changing workstation configurations such as screen savers, backgrounds, printers, BIOS information, preset passwords, etc.).
- Install software or download unauthorized files, games, programs, or other electronic media. Attempt to hack or access sites, servers, or content not intended for my use.
- Attempt to circumvent school safety measures and filtering tools.
- Send spam, electronic chain letters, or other useless information.
- Waste limited resources such as disk space, printing capacity, and bandwidth.
- Post-personally identifying information about myself or others.
- Agree to meet in real life with someone that the student met online.

- Use technologies for illegal activities, to pursue information about such activities, or to access illegal materials (i.e. threats, instructions on how to perform an illegal act, child pornography, drug dealing, fake identifications, purchase of alcohol, gang activities, etc.)
- Plagiarize content found online or violate copyright laws.
- View, send, display, or use racist, discriminatory, profane, lewd, vulgar, rude, disrespectful, threatening, or inflammatory language, messages, or pictures.
- Share passwords with others or attempt to find out the password of others.
- Post false or damaging information about other people, the school system, or school organizations.
- Trespass in another user‘s work, folders, or files.
- Use system network resources for personal gain or commercial purposes. This is not intended to be an exhaustive list.
- Incur unauthorized financial obligations for the school or school system

Limitation of Liability / Disclaimers

The Calhoun County School System makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the Board‘s technology resources will be error-free or without defect. Although the Board employs filtering and other safety and security mechanisms and attempts to ensure their proper function, it makes no guarantees as to their effectiveness. The Board will not be responsible, financially or otherwise, for unauthorized transactions conducted or financial obligations incurred on the system network. The Board will not be responsible for damage or harm to persons, files, data, or hardware. Neither the school nor the Calhoun County Board of Education will be responsible for any damages or losses incurred, including but not limited to: loss of data resulting from delays or interruption of service; loss of data stored on system resources; damage to personal property used to access system resources; the accuracy, nature, or quality of information stored on system resources; or unauthorized financial obligations incurred through system-provided access. Further, even though the system will use technical or manual means to limit student access, these limits do not provide a foolproof means for enforcing the provisions of this policy.

Adoption of Rules and Procedures

The Superintendent or designee is authorized to develop additional or more specific rules, procedures, or guidelines regarding acceptable use of technology to facilitate implementation of this policy.

Search and Inspection of Technology Resources and Devices

All technology resources, including but not limited to network and Internet resources, accounts, email systems, computers, and other devices owned, leased, or maintained by the Board are the sole property of the Board. Authorized Board personnel may, at any time and without prior notice, access, search, examine, inspect, collect, or retrieve information of any kind from the Board's technology resources to determine if a user is in violation of Board policies or rules regarding access to and use of technology resources, for or in connection with any other matter or reason related to the safe and efficient operation and administration of the school system, or for any other reason not prohibited by law. In addition, any device (regardless of ownership) brought onto school grounds by a student is subject to immediate inspection when there is a reasonable suspicion that the contents or recent utilization of the device are in violation of any of the Board's policies, rules or regulations regarding access to and use of technology resources.

Violations of Acceptable Use Policy

Student use of the computer network, the Internet, and other technology resources is a privilege, not a right. Violations of this policy may have disciplinary repercussions, including, but not limited to, the following:

- Suspension or termination of the network, technology, or computer privileges
- Completion of online course regarding acceptable use or similar corrective or rehabilitative measures
- Loss of privilege of bringing personally-owned technology devices to school
- Notification of and/or conference with parents
- In-school detention, out-of-school suspension, suspension from the school bus, or other disciplinary actions as authorized by the Code of Student Conduct
- Financial accountability for damage or loss
- Legal action and/or prosecution

Staff and contract employees use of the computer network, the Internet, and other technology resources is a privilege, not a right. Violations of this policy may have disciplinary repercussions, including, but not limited to, the following:

- Verbal Warning
- Corrective action plan
- Loss of privileges
- Administrative leave
- Financial accountability

- Legal action or prosecution
- Termination

Email

Legal Risks

- Email is a school business or educational communication tool, and users are obliged to use this tool in a responsible, effective, and lawful manner. Email lends itself to a kind of informality yet, from a legal perspective, may have the same implications as would any written communication. Any email is discoverable in a due process situation or other legal action. In addition, any email exchanged by a school system employee is a public record. Other legal risks of email for Calhoun County Schools and/or their network users include the following:
    - Sending emails with any libelous, defamatory, offensive, racist or obscene remarks.
    - Forwarding emails with any libelous, defamatory, offensive, racist, or obscene remarks.
    - Transmitting or forwarding confidential information;
    - Forwarding or copying messages without permission or implied permission.
    - Knowingly sending an attachment that contains a virus that severely affects another network or other users.
- By following the guidelines in this document, the email user can minimize the legal risks involved in the use of email. If any user disregards the rules set out in these guidelines, the user will be fully liable and Calhoun County Schools will disassociate itself from the user as far as legally possible.
- Do not send or forward emails containing libelous, defamatory, offensive, racist or obscene remarks. If you receive an email containing libelous, defamatory, offensive, racist or obscene remarks, promptly notify your supervisor.
- Use caution if you forward a message without implied permission or without acquiring permission from the sender first, especially if it contains sensitive or private information.
- Do not forge or attempt to forge email messages.
- Do not send email messages using another person's or a bogus email account.
- Do not copy a message or attachment belonging to another user without the permission or implied permission of the originator.
- Do not disguise or attempt to disguise your identity when sending an email.

Best Practices

Calhoun County Schools considers email as an important means of communication and recognizes the importance of proper email content and of speedy replies in conveying a professional image and in delivering good service. The use of email in education, however, is proliferating and the precise legal issues regarding appropriate use are yet to be determined. We are confident that—

- Any email exchanged by school system employees about individual students is a public record.

- Any email pertaining to a particular student is discoverable in a due process situation or other legal action.
- The nature of email lends itself to impulsive, overly informal, and sometimes unprofessional communication.

Note: The Technology Director is authorized to monitor and report inappropriate behaviors to the employee's supervisor who will take appropriate disciplinary action. Any other reports of inappropriate behavior, violations, or complaints will be investigated and routed to the employee's supervisor for appropriate action. Violations may result in a loss of access and/or appropriate disciplinary action up to and including termination. When applicable, law enforcement agencies may be involved.

Therefore Calhoun County Schools urges users to adhere to the following guidelines:

Guidance on Email between School Employees and Parents/Guardians

- Examples of the generally appropriate use of email between school employees and parents/guardians:
    - Teachers invite parents to provide email addresses and then send out emails to those addresses reporting on classroom activities, projects, and assignments. These messages are generic and do not refer to specific students.
    - Teachers may initiate or respond to emails from a parent or guardian about a specific child, exchanging objective, not subjective information such as the student's attendance, participation, homework, and performance in class.
- Examples of inappropriate use of email between school employees and parents/guardians:
    - Using email to report on serious problems regarding individual students.
    - Using email to discuss confidential and sensitive matters, including:
    - Medical/psychiatric/psychological diagnoses and treatments.
    - Contents of special education and/or Section 504 evaluations, intervention plans, IEPs, 504 plans, disciplinary matters.
    - Family problems and other sensitive family information.
    - Using language that is subjective, judgmental, unprofessional, pejorative, and/or labeling. Examples:
        - "Have you considered that Johnny might have ADHD?"
        - "Overall, I think that Johnny is unmotivated/lazy."
        - "I don't think there is anything wrong with Johnny except his negative attitude."
        - "I think this child's problem is his home life."
- Email between teachers and parents shall be positive and/or general in nature when possible. Discussions involving serious problems and any and all protected information (medical, psychological, psychiatric, Special Education, and Section 504, and disciplinary matters) should occur in person or by telephone.

- Parents may initiate inappropriate email exchanges. Example: “Johnny is in your American History class and is failing. His father is an alcoholic and we are divorced. Johnny has ADHD and clinical depression. Can you please tell me how he is doing in your class and what I can do to help him?”
    - That kind of message shall be deleted and the teacher receiving it should call the parent who sent it. Alternatively, the teacher could reply to it, deleting everything from the body of the email sent by the parent, and then respond with directions about how the teacher can be reached by telephone or in-person. Do not regard a parent or guardian’s initiation of this kind of email exchange as constituting permission for you to discuss these matters via email.

General Best Practices involving all email are as follows:

Writing emails:

- Use short, descriptive Subject: lines.
- Avoid lengthy, detailed email messages. Consider using an attachment for “How To” information, directions, procedures, processes, or similar types of information.
- Avoid unnecessary attachments or large file attachments such as multiple pictures, mini-movies, etc. AVOID USING ALL CAPITALS.
- If using cc or bcc features, take steps to inform the cc or bcc recipient of any action expected unless the action is explicit in the email. The bcc option is often used to avoid revealing recipient email addresses to the entire group receiving the email; otherwise, the bcc option shall be used sparingly if at all.
- If you forward emails, state clearly what action you expect the recipient to take.
- Use the spell checker before you send out an email.
- If the content of an email is not of a public nature, consider using another form of communication or protect the information by using a password.
- Only mark emails as important if they really are important.

Replying to emails:

- Emails shall be answered within 24 hours, and at minimum employees are expected to check email at least once per day.
- Responses shall not reveal confidential information and shall be professional.

Electronic Social Networking, Instant Messaging including Texting, etc.

- Electronic social networking and/or instant messaging, such as but not limited to Twitter, IM, or texting, among staff and students, is a particularly sensitive matter in a time when growing numbers of school employees maintain social networking accounts, email extensively in their personal lives, and are accustomed to using instant messaging services.
- An absolute prohibition of communicating electronically with students seems excessive. On the other hand, teachers and school staff shall maintain the highest standards should they choose to

interact with students through electronic media. Below are some typical situations in which employees might need guidance.

- The guidelines below are presented in a Q&A format.
  - Q: Is it ok for me to initiate electronic communications with a student?
  - A: If a teacher initiates overly personal contact with students outside of school, whether in person or electronically, he or she may create an impression of an unhealthy interest in that student's personal life and may leave himself or herself open to an accusation of inappropriate conduct. Therefore, caution shall be exercised in this type of communication.
  - Q: What if I receive an email or other electronic message such as a text from a student?
  - A: This very much depends on the nature of the communication received. We would strongly discourage any use of texting, instant messaging, or "chat"-type communication with students for purposes other than school-related communications. Do not engage in social "chat" with students. If a communication is received which appears to be a social greeting, you might do best just to acknowledge it in an appropriate way at school. A very brief acknowledging electronic response might be appropriate in some circumstances. However, it is perfectly OK not to respond to such greetings. If you choose to not respond, making an extra effort to cheerfully greet the student at school might be appropriate.
- If a student sends a message with disturbing content, you should discuss this with your administrator or supervisor, including a school counselor in the discussion as needed.
- If a student sends a message that appears to suggest an emergency (an allegation of abuse or a student sharing suicidal thoughts or plans), try to contact your administrator or supervisor at once.

- Q: What about Facebook accounts or other social networking sites? Should I respond to an invitation to become a student's "Friend"?
- A: We recommend that you not engage in online social networking with students unless the site is used for school information or academic reasons only. This would only be an issue, of course, if you choose to maintain a Facebook, or similar account. If you do so, we recommend that you be extremely cautious about the content of your profiles and pages. If you are strictly using a social networking site for school-related topics and stay away from personal content then these sites shall be treated much like any other educational blog. (However, the use of comments, "writing on walls," and so on, would be likely to lead to major problems if an approval process is not in place before posting.) You may find that it is easier to simply tell your students that you have a policy not to accept students as "friends."

General Email Information

- Virus Protection and Filtering
  - Incoming and outgoing emails sent to or received from Calhoun County Schools' Exchange email server are scanned for viruses, spam, and content. However, users are

expected to exercise caution when opening emails from unknown users or when using the web-based email client from home computers.

- Incoming emails may be blocked if the message size is over 100,000 KB or if there are multiple attachments.

Disclaimer

- Calhoun County Schools recommends that employees add a disclaimer to outgoing emails or automatically attach a disclaimer such as the one below to each email sent outside the school system.
- "This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to which they are addressed. If you have received this email in error please notify the system manager. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the Calhoun County Schools. Finally, the recipient should check this email and any attachments for the presence of viruses. The company accepts no liability for any damage caused by any virus transmitted by this email."

System Monitoring

- Although Calhoun County Board policy permits personal use of school email accounts, users shall have no expectation of privacy in anything they create, store, send or receive on the Calhoun County Schools' computer system. Emails may be monitored without prior notification if Calhoun County Schools deems this necessary. If there is evidence that users are not adhering to the guidelines set out in this policy, Calhoun County Schools reserves the right to take disciplinary action, including termination and/or legal action.

Email Accounts

- Email accounts are assigned to new employees when their employment is approved by the Board of Education and when the new employee has read and signed the Acceptable Use Policy and has an understanding of the Acceptable Use Policy. All email accounts maintained on the Calhoun County email and Internet communication systems are property of Calhoun County Schools. Calhoun County maintains student accounts and employee accounts.
- Passwords shall not be given to other people and shall be changed if the user believes his/her password is no longer secure. Email accounts are deleted immediately when employees retire, resign, or take leave from the school system for a period of six months or more. Only Calhoun County employees are given email accounts. Upon request by the administration, Calhoun County employee-sponsored accounts, such as PTA accounts or accounts for contract employees may be created. Employer-sponsored accounts are subject to these guidelines and it is the responsibility of the sponsoring employee to educate the user of this and all other relevant technology-related policies and guidelines.
- Email is not to be utilized by employees to share confidential information about students or other employees. Email messages are not entirely secure and should not be considered private.

Messages may sometimes be diverted accidentally to a destination other than the one intended. Privacy in these communications is not guaranteed. The district reserves the right to access stored records in cases where there is reasonable cause for misuse.

Electronic Communications for Personal Use

- Although Calhoun County Schools' email and Internet communication systems are meant for school business, Calhoun County Schools allow the reasonable use of email for personal use if certain guidelines are adhered to:
    - Personal use of email shall not interfere with work.
    - Personal emails shall also adhere to the guidelines in this policy.
    - Personal emails shall be deleted regularly so as not to clog the system.
- The forwarding of chain letters, junk mail, inappropriate jokes, and executable files is strictly forbidden.
    - Do not send personal mass mailings.
    - Do not send emails for personal gain, to solicit business for friends, family, etc., or for political purposes.
    - All messages distributed via the school system's email and Internet communication systems, even personal emails, are Calhoun County Schools' property.
    - Recognize the diversity of co-workers when sending emails. For example, some employees would regard emails of a religious nature, including invitations to religious events or services – even prayer requests – as inappropriate or offensive.

Questions

- If you have any questions or comments about these guidelines, please contact your principal or immediate supervisor. If you do not have any questions Calhoun County Schools presume that you understand and are aware of the rules and guidelines and will adhere to them.