# CALHOUN CUSD 40 DISTRICT WEB SITE

The Calhoun Unit 40 Web Site is developed, operated and maintained as a closed forum to provide community access to information about the district and its programs/activities.

The Calhoun Unit 40 Board of Education will make every effort to protect students and staff from hazards associated with the district's Web Site. The district will not publish or provide for publication any personal student information without first obtaining the written approval of that student's parents. Personal information shall mean any information that identifies a student, including, but not limited to the student's full name, photograph, personal biography, e-mail address, home address, date of birth, social security number and parent's name.

The district shall require that information on the Web Site be well written, adequately researched, unbiased/unprejudiced and apply appropriate language, suitable for audiences of all age levels.

All Web Pages created by students and student organizations on the district computer system will be subject to treatment as district-sponsored publications.

Linked sites, available through the district Web Site are not under the control of the district. The district is not responsible for the contents of any site or any link contained in a linked site, or any changes or updates to such sites. The district provides links as a convenience, and the inclusion of any link does not imply endorsement of the site by the district.

The Superintendent shall be responsible for overseeing the implementation of this policy and accompanying rules.

The Calhoun Unit 40 Board of Education expressly reserves the right to limit, revise or eliminate any information provided on the Web Site.

## CALHOUN UNIT 40 ELECTRONIC ACCESS

The Calhoun Unit 40 electronic communications systems are developed, operated, and maintained as part of the school district information and communication infrastructure. The purpose of these systems is to provide internal and external communication to promote increased educational opportunities for staff, students and the community.

The Calhoun Unit 40 Board of Education strongly believes in the educational value of electronic communication services and recognizes their potential support to curriculum and student learning. The goal for providing this service is to promote educational excellence.

The Calhoun Unit 40 Board of Education will make every effort to protect students and teachers for misuses or abuses as a result of their experiences with the electronic services. All users and contracted service providers shall adhere to board policies, federal and state laws/regulations when accessing or producing electronic services. The Calhoun Unit 40 Board of Education recognizes that on a global network it is impossible to control all materials. The District firmly believes that the valuable information and interaction available on this worldwide network far outweighs the possibility of users procuring material that is not consistent with the education goals within each school.

Our School District has the ability to enhance your child's education through the use of electronic networks, including the Internet. Our goal in providing this service is to promote educational excellence by facilitating resource sharing, innovation, and communication. Students and their parents/guardians need only sign this Authorization for Access to the District's Electronic Networks once while the student is enrolled in the School District.

The District filters access to materials that may be defamatory, inaccurate, offensive, or otherwise inappropriate in the school setting. If a filter has been disabled or malfunctions it is impossible to control all material and a user may discover inappropriate material. Ultimately, parents/guardians are responsible for setting and conveying the standards that their child should follow, and the School District respects each family's right to decide whether or not to authorize Internet access.

With this educational opportunity also comes responsibility. The use of inappropriate material or language, or violation of copyright laws, may result in the loss of the privilege to use this resource. Remember that you are legally responsible for your child's actions. If you agree to allow your child to have a network account, sign the Handbook/Authorization form below and return it to your school.

Students and parents will be informed via the District's Acceptable Use/Permission Form that the following activities are not permitted on the District's computers.

1. Access to material that is inappropriate in the school environment.
2. Behaviors that reduce or negatively impact the safety and security of the students when using electronic mail, chat rooms and other forms of direct electronic communications.
3. Unauthorized access, including "hacking" and other unlawful activities.
4. Unauthorized disclosures, use, and dissemination of student personal information.
5. Overriding, or disabling district filtering measures by anyone other than the District's authorized designee.

Inappropriate use or abuse of the communication systems will result in disciplinary action, ad may result in banning the user/provider permanently from the communication service.

Calhoun Unit 40 Board of Education expressly reserves the right to limit, revise or eliminate any electronic services provided to any user in the system.

# AUTHORIZATION FOR INTERNET AND COMPUTER NETWORK ACCESS
# CALHOUN CUSD # 40

All use of the Internet (and all services accessed through our Internet connection) shall be consistent with the Board of Education's goals of promoting educational excellence by facilitating resource sharing, innovation, and communication. The Superintendent or designee shall develop an implementation plan for this policy and appoint a system administrator.

School Board members, students, support staff, and administrators shall be held to the same procedures for the purpose of this *Authorization*. Please read this document carefully before signing. This *Authorization* does not attempt to state all required or prescribed behavior by users. However, some specific examples are provided. The failure of any user to follow the terms of the *Authorization* for Internet access will result in loss of privileges, disciplinary action, and/or appropriate legal action. The signature(s) at the end of this document is legally binding and indicates the party who signed has read the terms and conditions carefully and understands their significance.

Terms and Conditions:

The term electronic networks includes all of the District's technology resources, including, but not limited to:

The District's local-area and wide-area networks, including wireless networks (Wi-Fi), District-provided Wi-Fi hotspots, and any District servers or other networking infrastructure;

Access to the Internet or other online resources via the District's networking infrastructure or to any District-issued online account from any computer or device, regardless of location;

District-owned and District-issued computers, laptops, tablets, phones, or similar devices.

Acceptable Use – Access to CUSD 40's Internet must be for the purpose of education or research, and be consistent with the educational goals and objectives of the District.

Privileges – The use of CUSD 40's Internet is a privilege, not a right, and inappropriate will result in cancellation of those privileges. The Superintendent, Building Principal, or System Administrator will make all decisions regarding whether or not a user has violated this Authorization and may deny, revoke, or suspend access at this time.

Unacceptable Use – You are responsible for your actions and activities involving the District's computer network. Some examples of unacceptable uses and practices are:

Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any U.S. or State regulation;

Unauthorized downloading of software, regardless of whether it is copyrighted or de-virused;

Using the internet for private financial or commercial gain;

Wastefully using resources, such as file space;

Gaining unauthorized access to resources or entities;

Hacking or attempting to hack or gain unauthorized access to files, accounts, resources, or entities by any means

Invading the privacy of individuals; including the unauthorized disclosure, dissemination, and use of information about anyone that is personal, such as a photograph or video;

Using another user's account or password – NOTE: Do NOT give out your password, except on request of the building Principal or System Administrator. If you suspect that someone knows your password, see the System Admin. to have it changed immediately. You are responsible for ALL activity on your account;

Posting material authored or created by another without his/her consent;

Using the network for commercial or private advertising;

Posting anonymous messages;

Posting or sending anonymous messages;

Creating or forwarding chain letters, spam, or other unsolicited messages;

Using the electronic networks for commercial or private advertising

Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, bullying, racially offensive, harassing, or illegal material that is harmful to children will be a direct violation of this policy;

Behaviors that reduce or negatively impact the safety and security of individuals when using electronic mail, chat rooms, Twitter, Facebook, other social media sites, and other forms of direct electronic communications;

Misrepresenting the user's identity or the identity of others;

Using the network while accesses to privileges are suspended or revoked;

Unauthorized access, including "hacking" and other unlawful activities;

Using the electronic networks to engage in conduct prohibited by board policy

Security – Network security is a high priority. If you identify a security problem on the network you must notify the system administrator. Keep your account information and password confidential. Do not use another individual's account. Attempts to log in to the network as a system administrator will result in the cancellation of user privileges. Overriding, or disabling district filtering measures by anyone other than the District's authorized designee is strictly forbidden. Any user identified as a security risk may be denied access to the network.

Use of E-Mail – The District's email system, and its constituent software, hardware, and data files, are owned and controlled by the School District. The School District provides email to aid students as an education tool.

The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any student or staff member to an email account is strictly prohibited.

Each person should use the same degree of care in drafting an electronic mail message as would be put into a written memorandum or document. Nothing should be transmitted in an e-mail message that would be inappropriate in a letter or memorandum.

Electronic messages transmitted via the school district's Internet gateway carry with them an identification of the user's Internet "domain." This domain name is a registered domain name and identifies the author as being with the school district. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of the school and district. Users will be held personally responsible for the content of any and all electronic mail messages transmitted to external recipients.

Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the system administrator. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.

Use of the School District's email system constitutes consent to these regulations.

Electronic communications such as email, site access history, and downloaded material may be monitored or read by school officials.

Vandalism – vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.

No warranties – CUSD 40 makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages you suffer. This includes loss of data resulting from delays, non-delivered data, software or hardware failure, or service interruptions caused by its negligence or your errors or omissions. Use of any information obtained via the internet is at your own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Indemnification – The user agrees to indemnify CUSD 40 for any losses, cost, or damages, including reasonable attorney fees, incurred by the District relating to, or arising from, any breach of this Authorization.

Users are NOT to download or install any executable files or any operating system or software upgrades on Unit 40 workstations without the prior permission of the System Administrator.

ACCESS TO STUDENT SOCIAL NETWORKING PASSWORDS AND WEBSITES: Parents and students are hereby notified that school authorities may request or require a student to provide a password or other related account information in order to gain access to the student's account or profile on a social networking website if school authorities have reasonable cause to believe that the student's account on a social networking website contains evidence that the student has violated a school disciplinary rule or policy. Parents and students are further notified of the following: (a) a student's refusal to provide a password or other related account information upon request shall subject the student to discipline; and (b) a student's refusal to provide a password or other related account information upon request shall be deemed by school authorities and the Board of Education as an admission by the student that he/she has violated a school disciplinary rule or policy. "Social networking website" means an Internet-based service that allows individuals to do the following: (a) construct a public or semi-public profile within a bounded system created by the service; (b) create a list of other users with whom they share a connection within the system; and (c) view and navigate their list of connections and those made by others within the system.

Network Etiquette - The user is expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

Be polite. Do not become abusive in messages to others.

Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.

Do not reveal personal information, including the addresses or telephone numbers, of students or colleagues.

Recognize that electronic mail (e-mail) is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.

Do not use the network in any way that would disrupt its use by other users.

Consider all communications and information accessible via the network to be private property.

All students, faculty, support staff, and administration will be trained annually on the safe use of the Internet.

Each student (parent/guardian), teacher, staff member, Board member, and Administrator must sign the District's Authorization for Internet and Computer Network Access as a condition for using the District's Internet connection and computer network on an unsupervised basis.

By signing the Parent/Guardian & Student Handbook Acknowledgement/Internet & Network Authorization sheet on the last page of this handbook, I agree to the above policy and (for parents); give authorization for my son/daughter to access the District's computer network and Internet.

No Warranties – The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Indemnification – By using the District's electronic networks, the user agrees to indemnify the District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any violation of these procedures.

Security – Network security is a high priority. If the user can identify or suspects a security problem on the network, the user must promptly notify the system administrator or Building Principal. Do not demonstrate the problem to other users. Keep user account(s) and password(s) confidential. Do not use another individual's account without written permission from that individual. Attempts to log-on to the network as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the networks.

Vandalism – Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of malware, such as viruses and spyware.

Telephone Charges – The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, texting or data use charges, long-distance charges, per-minute surcharges, and/or equipment or line costs.

Copyright Web Publishing Rules – Copyright law and District policy prohibit the re-publishing of text or graphics found on the Internet or on District websites or file servers/cloud storage without explicit written permission.

For each re-publication (on a website or file server) of a graphic or a text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the web address of the original source.

Students engaged in producing web pages must provide library media specialists with email or hard copy permissions before the web pages are published. Printed evidence of the status of public domain documents must be provided.

The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the website displaying the material may not be considered a source of permission.

The fair use rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.

Student work may only be published if there is written permission from both the parent/guardian and student.

Use of Email – The District's email system, and its constituent software, hardware, and data files, are owned and controlled by the District. The District provides email to aid students in fulfilling their duties and responsibilities, and as an education tool.

The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any student to an email account is strictly prohibited.

Each person should use the same degree of care in drafting an email message as would be put into a written memorandum or document. Nothing should be transmitted in an email message that would be inappropriate in a letter or memorandum.

Electronic messages transmitted via the District's Internet gateway carry with them an identification of the user's Internet domain. This domain is a registered name and identifies the author as being with the District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of the District. Users will be held personally responsible for the content of any and all email messages transmitted to external recipients.

Any message received from an unknown sender via the Internet, such as spam or potential phishing emails, should either be immediately deleted or forwarded to the system administrator. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.

Use of the District's email system constitutes consent to these regulations.

Internet Safety

Internet access is limited to only those acceptable uses as detailed in these procedures. Internet safety is supported if users will not engage in unacceptable uses, as detailed in these procedures, and otherwise follow these procedures.

Staff members will supervise students while students are using District Internet access to ensure that the students abide by the Terms and Conditions for Internet access contained in these procedures.

Each District computer with Internet access has a filtering device that blocks entry to visual depictions that are: (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee.

The system administrator and Building Principals shall monitor student Internet access.

## Cell Phones/Electronic Communication Devices:

All students must follow district policies and procedures regarding cell phone/other electronic communication devices possession or usage on school property, including school buses. The policies and procedures must be strictly adhered to and are as follows:

- "The school administration is authorized to discipline students for gross disobedience or misconduct

regarding the use or possession of a cell/smart phone, electronic signaling device, a two-way radio, video recording device, and/or other telecommunication device, unless authorized and approved by the Building Principal." (School Board of Education Policy 7:190)

- Cyber Bullying: Any communication or materials created OUTSIDE of school that are discussed, distributed or brought into the school setting or that substantially interfere with or disrupt the educational process are subject to disciplinary action.

- Students who bring electronic communication devices to the school building/grounds during school hours MUST keep them turned off, in their book bag, and stored inside their assigned lockers during the school day. The building principal may grant permission to allow students to use their cell/smart phones, iPads, iPods, etc. for specific reasons and when deemed appropriate. Administrative permission must be requested in advance by the students' teacher.

- Students may be disciplined for sending, receiving or possessing sexually explicit or otherwise inappropriate pictures or images, commonly known as "sexting."

- *** Students who violate the above procedures will be required to turn in their device to the teacher/administrator and parents/guardians will be contacted to pick up the device. It will not be returned to the student. Students may not be allowed to bring devices to school for a period of time—dependent upon the severity and number of violations. This will be according to the administrator's discretion.