



Dear Parent or Guardian:

Carthage E.S.D. #317 is using Chromebooks this school year. To help keep your child safer and more scholarly online, we have adopted online services provided by GoGuardian.

It may be helpful to know that over 10,000 other schools use GoGuardian to protect 5.5 million students across the world, and the [Global Educator Institute](#) has endorsed the GoGuardian Teacher product.

How are we using GoGuardian?

We have chosen GoGuardian Admin and GoGuardian Teacher services to:

- Help protect students against harmful and inappropriate online material
- Help students stay "scholarly" and more focused when learning online
- Helping assess students' progress towards class assignmentsFacilitating communication between teachers and students during class time

When and how does GoGuardian operate?

GoGuardian's web-based services operate on our school's managed Google Suite for Education Chrome accounts (i.e., when a student is logged into Chrome or a Chromebook

What are the school's responsibilities?

Carthage E.S.D. #317 selected GoGuardian services to help our students stay safer and more scholarly online. We will work with students during class time to help teach them digital responsibility and safety. Additionally, we will train teachers about how to operate GoGuardian and about our policies and procedures to help protect student privacy.

What are my parental/guardian and child's responsibilities?

We ask that students uses their school-managed Google accounts and school-managed devices for educational purposes within the boundaries of Carthage E.S.D.'s Acceptable Use Policy/Authorization for Internet Access agreement.

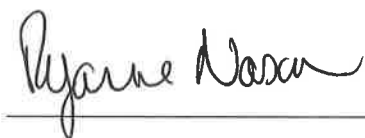
When a student is off campus, parents are responsible for supervising internet access and usage. We encourage you to discuss rules for appropriate internet usage with your child, and reinforce lessons of digital citizenship and safety with him or her. We also highly encourage you to report any potential cyberbullying or other sensitive issues to us.

How does GoGuardian help protect my child's privacy?

To help your child remain scholarly and safe online, GoGuardian collects certain personally identifiable information about your child. GoGuardian has consulted with privacy experts, participates in privacy organizations, is a proud signatory of the Student Privacy Pledge, and has been awarded certifications by iKeepSafe for complying with both Family Education Rights and Privacy Act and California student privacy laws. For more detailed information about GoGuardian, you may visit GoGuardian's website, Trust & Privacy Center, GoGuardian's Product Privacy Policy, and the attached COPPA Notice and Disclosure Form.

We are here to answer any questions that you may have.

Sincerely,

A handwritten signature in cursive script, reading "Ryanne Nason", positioned above a horizontal line.

Miss Ryanne Nason
CMS Principal/CESD Special Education Director

Access to Student Social Networking Passwords & Websites

School officials may conduct an investigation or require a student to cooperate in an investigation if there is specific information about activity on the student's account on a social networking website that violates a school disciplinary rule or policy. In the course of an investigation, the student may be required to share the content that is reported in order to allow school officials to make a factual determination.

Due Process Rights of Students

Individual rights granted by the Constitution of the United States are granted to all people regardless of age, sex, color, or creed. Students have rights as individuals. The school disciplinary procedures should not violate these rights. The essential rights involved in disciplinary procedures stem from the concept of due process. A student is entitled to:

- Know what the rules and regulations are.
- Know what charges are brought against him or her.
- Present his or her point of view and/or evidence about the charges.
- Have a notice of and hearing on the charges.
- Have counsel.
- Appeal a decision regarding the charges to a higher level.
- Have the charges or penalties removed from the record if the evidence demonstrates his or her innocence or non-involvement.

In the administration of the discipline procedures outlined in this handbook, the student should be made to feel that he or she is valued as a person. It is his or her behaviors that are in question.

Section 7 – Internet, Technology & Publications

Acceptable Use Policy/Authorization for Internet Access

All use of the Internet shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation and communication. This *Authorization* does not attempt to state all required or proscribed 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 the loss of privileges, disciplinary action and/or appropriate legal action. The signature(s) at the end of this document is legally binding and indicated the party who signed has read the terms and conditions carefully and understands their significance.**

The smooth operation of the network relies upon the proper conduct of the end-users who must adhere to strict guidelines. These guidelines are provided so that you are aware of the responsibilities you are about to acquire. In general, your responsibilities require efficient, ethical and legal utilization of the network or the network resources. Each student applying for an account will participate in a discussion with his or her sponsoring teacher regarding proper behavior and use of the network. The signature(s) at the end of this document is (are) legally binding and indicate(s) the party(s) who has (have) read the terms and conditions carefully and understand(s) their significance and agree(s) to abide by these terms.

Terms and Conditions

1. Privileges - The use of the District's Internet is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges, disciplinary action and/or referral to legal authorities. The building principal may deny, revoke or suspend access at any time.
2. Acceptable Use - Access to the District's Internet must be for the purpose of education or research, and be consistent with the educational objectives of the District. Carthage Community District Network users are responsible for all activities through their point of access.
 - a) Responsible users may receive the privilege of having free Internet access upon completion of proper forms and participation in a discussion with a sponsoring teacher regarding proper behavior and use of the network.

- b) Keep assigned Internet access as long as the user is a staff member, member of the Board of Education, or student in the Carthage Community District or a retired member of the staff.
 - c) Carthage Community District Network users should change their password frequently and must not give a password to another user.
 - d) Responsible users may use the Internet to research assigned classroom projects.
 - e) Responsible users may use the Internet to send electronic (e-mail) to other users via an approved school-provided email account.
 - f) Responsible users may use the Internet to explore other computer systems.
 - g) Any Carthage Community District Network user's traffic that traverses another network may be subject to that network's acceptable use policy.
3. Network Etiquette - You are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:
- a) Be polite; do not become abusive in your messages to others.
 - b) Use appropriate language. Do not swear or use vulgarities or any other inappropriate language.
 - c) Do not reveal personal information, including the addresses or telephone numbers of students or colleagues.
 - d) 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.
 - e) Do not use the network in any way that would disrupt its use by other users.
 - f) Consider all communications and information accessible via the network to be private property.
 - g) Electronic bullying, hate mail, harassment, discriminatory remarks and other antisocial behaviors are prohibited on the network. Therefore, messages should not contain threats, profanity, obscene comments, sexually explicit material, and expressions of bigotry or hate.
 - h) Subscriptions to Listservs must be reported to a system administrator. Prior approval for Listservs is required for students.
 - i) Mail Listservs must be monitored daily and deleted from the personal mail directory to avoid excessive use of fileserver hard-disk space.
 - j) Time and bandwidth are costly. While accessing the Internet, no games (e. g. MUD's) may be played.
 - k) From time to time, Carthage Community District administrators will make determinations on whether specific uses of the network are consistent with the acceptable use policy
4. Unacceptable Use - The user is responsible for his or her actions and activities involving the network. Some examples of unacceptable uses are:
- a) 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.
 - b) Unauthorized downloading of software, regardless of whether it is copyrighted or de-virused.
 - c) Downloading copyrighted material for other than person use.
 - d) Using the network for private financial or commercial gain.
 - e) Wastefully using resources, such as file space.
 - f) Hacking or gaining unauthorized access to resources or entities.
 - g) Invading the privacy of individuals, which includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature.
 - h) Using another user's account or password.
 - i) Posting material authored or created by another without his/her consent.
 - j) Posting anonymous messages.
 - k) Using the network for commercial or private advertising.
 - l) Accessing, submitting, posting, publishing or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing or illegal material.
 - m) Using the network while access privileges are suspended or revoked.
5. 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 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.

Because access to the Internet provides connections to other computer systems located all over the world, users (and parents of users who are students) must understand that neither the Carthage Community District nor any District staff member controls the content of the information available on these other systems.

Some of the information available is controversial and, sometimes, may be offensive. The Carthage Community District does not condone and is not liable for the use of such materials.

6. Indemnification - The user agrees to indemnify the School District for any losses, costs or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any breach of this *Authorization*.
7. Security - Security on any computer system is a high priority, especially when the system involves many users. If you feel you can identify a security problem on the Internet, you must notify an administrator or faculty member. Do not demonstrate the problem to other users. Do not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users. Do not use another individual's password, forge messages or post anonymous messages. Attempt to gain unauthorized access to system programs or computer equipment will result in cancellation of user privileges. Attempts to login to the system as a system administrator or any other form of unauthorized access will result in immediate cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to school computers.
8. The security of computer systems is based to a great extent on passwords. Therefore, it is important to take your password very seriously, and to keep it secret at all times. Do not select an obvious password, and have your password changed any time there is any chance that someone else may have learned it. If someone else accesses the network using your password, you could be held responsible for any actions they make. Your password is for your protection. It ensures that no one can make unauthorized use through your means of access. Use of any other user's password or loaning the use of your password is prohibited. Do not attempt to steal or use any other person's password or account, even for fun or as a joke.
9. Vandalism - Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy computer hardware, data of another user, the Internet or any other computer programs. This includes, but is not limited to, the uploading or creation of computer viruses, contamination, deletion or reconfiguration of data or degradation of system performance in any way.
10. Telephone Charges - The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges and/or equipment or line costs.
11. Copyright Web Publishing Rules-Copyright law and District policy prohibit the re-publishing of text or graphics found on the Web or on District Web sites or file servers, without explicit written permission.
 - a) For each re-publication (on a Web site 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.
 - b) Students and staff engaged in producing Web pages must obtain a hard copy of the policy Exhibit 7:340-E-- Using a Photograph or Videotape of a Student permission form from the superintendent's designee before the Web pages are published. Printed evidence of the status of "public domain" documents must be provided.
 - c) 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 Web site displaying the material may not be considered a source of permission.
 - d) The "fair use" rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.
 - e) Student work may only be published if there is written permission from both the parent/guardian and student.
12. Use of Electronic Mail
 - a) The District's electronic mail system, and its constituent software, hardware, and data files, are owned and controlled by the School District.
 - b) The school will not permit the use of any form of Internet-based email (i.e. Hotmail, Yahoo mail, AOL mail, etc.) An Internet filtering device will block access to all student and staff use of Internet-based email, with the exception of school-sponsored staff email accounts, which are to be used for school-related business purposes.

- c) The School District may provide e-mail to aid students and staff members in fulfilling their duties and responsibilities, and as an education tool.
- d) 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 electronic mail account is strictly prohibited.
- e) 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.
- f) 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 this School District. Users will be held personally responsible for the content of any and all electronic mail messages transmitted to external recipients.
- g) 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 electronic mail system constitutes consent to these regulations.

13. Internet Safety

- a) Internet access is limited to only those "acceptable uses" as detailed in these procedures. Internet safety is almost assured if users will not engage in "unacceptable uses," as detailed in this *Authorization*, and otherwise follow this *Authorization*.
- b) Staff members shall 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 this *Authorization*.
- c) Each District computer with Internet access has a filtering device that blocks entry to 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.
- d) The system administrator and Building Principals shall monitor student Internet access.

All users of the District's computers and means of Internet access shall maintain the confidentiality of student records. Reasonable measures to protect against unreasonable access shall be taken before confidential student information is loaded onto the network.

Students, parent(s)/guardian(s) and teachers must sign this *Authorization for Internet Access* on or before the start of each school year while enrolled or employed by the School District.

Guidelines for Student Distribution of Non-School-Sponsored Publications

A student or group of students seeking to distribute more than 10 copies of the same material on one or more days to students must comply with the following guidelines:

1. The student(s) must notify the building principal of the intent to distribute, in writing, at least 24 hours before distributing the material. No prior approval of the material is required.
2. The material may be distributed at times and locations selected by the building principal, such as, before the beginning or ending of classes at a central location inside the building.
3. The building principal may impose additional requirements whenever necessary to prevent disruption, congestion, or the perception that the material is school-endorsed.
4. Distribution must be done in an orderly and peaceful manner, and may not be coercive.
5. The distribution must be conducted in a manner that does not cause additional work for school personnel. Students who distribute material are responsible for cleaning up any materials left on school grounds.
6. Students must not distribute material that:
 - a. Will cause substantial disruption of the proper and orderly operation and discipline of the school or school activities;
 - b. Violates the rights of others, including but not limited to, material that is libelous, invades the privacy of others, or infringes on a copyright;