GRANDVIEW ISD
2017 - 2018 ACCEPTABLE USE POLICY FOR STUDENTS

A goal of Grandview ISD is to promote innovation and educational excellence in the Grandview public schools. It is imperative that students conduct themselves in a responsible, decent, ethical, and polite manner while using the network. Grandview ISD 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.

Students will be able to bring their own technology devices (laptops, notebooks, smart phone, etc.) for use in the school setting. Each teacher will set their own policies regarding technology use in their classroom. Some may allow it freely. Some may allow it at certain times. Some may not allow it at all. Students are expected to adhere to each teacher's individual policy regarding technology use.

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.

- The Grandview ISD network is intended for educational purposes.
- All activity over the network or 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.
- Misuse of school resources can result in disciplinary action.
- Grandview ISD 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 use of school technologies.
- Users of the district network or other technologies are expected to alert IT staff immediately of any concerns for safety or security.

Technologies Covered

Grandview ISD may provide Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, access to the Grandview ISD Wi-Fi network, and other available resources.

As new technologies emerge, Grandview ISD 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.

Usage Policies

All technologies provided by the district are intended for educational 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; don't try to get around technological protection measures; use good common sense; and ask if you don't know.

The student in whose name an account is issued will be responsible for its proper use. Students shall not allow others to use their username and password nor use another person's log-on information.

Students shall not use computers for any non-instructional purposes (games, chat rooms, music/video downloads, personal email, etc). Student use of computers and the network (whether the device is district owned or personal) is only allowed when supervised by a staff member. Any deliberate attempt to harm or destroy district equipment or another student's device or materials is prohibited. Grandview SD is not responsible for any lost, damaged or stolen personal devices.

Web Access

Grandview ISD provides its users with access to the Internet, including web sites, resources, content, and online tools. That access will be restricted in compliance with CIPA regulations and school policies. Web browsing is 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 their teacher or an IT staff member.

Email

Grandview ISD may provide users with email accounts for the purpose of school-related communication. Availability and use will be restricted based on school policies.

School email accounts should be used with care. Users should not send personal information; should not attempt to open files or follow links from unknown or untrusted origin, should use appropriate language, and should only communicate with other people as allowed by the district policy or the teacher.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage will be monitored and archived.

Social/Web 2.0 / Collaborative Content

Recognizing the benefits collaboration brings to education, Grandview ISD will provide users with access to web sites 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 will be monitored. Users should be careful not to share personally-identifying information online.

Personally-Owned Devices Policy

Students should keep personally-owned devices (including laptops, tablets, smart phones, and cell phones) turned off and put away during class time—and only use them as instructed by a teacher or staff for educational purposes. As referenced on page 30 of the Student Handbook: Students are prohibited from possessing, sending, forwarding, posting, accessing, or displaying electronic messages, pictures or videos that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal. This prohibition also applies to conduct off school property, whether the equipment used to send such messages is district-owned or personally owned, if it results in a substantial disruption to the educational environment.

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 untrusted origin.

Deliberate attempts to bypass security, firewall, and filter systems or to tamper with system performance or equipment will be viewed as violation of district guidelines and possibly as criminal activity under state law (Texas Penal Code, Computer Crimes, Chapter 33).

If students suspect a computer or mobile device they are using might be infected with a virus, they should alert a staff member or IT. Students should not attempt to remove the virus or download any programs to help remove the virus

Downloads

Users should not download or attempt to download or run .exe programs over the school network or onto school resources without express permission from IT staff.

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 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 wouldn't 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 that were never intended.

Plagiarism

Users should cite sources for all content with copyright from the Internet including words, images, videos, and music.

Personal Safety

A student should never share personal information, including phone number, address, social security number, birthday, or financial information over the Internet without adult permission. Users should recognize that communicating over the Internet brings anonymity and associated risks and should carefully safeguard their personal information and that of others. Users should never agree to meet an online acquaintance in real life without parental permission.

If a student sees a message, comment, image, or anything else online that makes him/her concerned for his/her personal safety, the student should immediately bring it to the attention of an adult (teacher or staff at school, parent if at home).

Cyber Bullying

Cyber bullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyber stalking are all examples of cyberbullying. Students should not send emails or post comments 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 severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Remember online activities are monitored and retained.

Limitation of Liability

While Grandview ISD employs filtering and other safety and security mechanisms and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.

Grandview ISD will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

Grandview ISD will not be responsible for damage or harm to persons, files, data, or hardware on personally owned devices.

Please sign and date the last page and return to your campus secretary as soon as possible. Please retain the first two pages for your reference.

Violations of this Acceptable Use Policy

Information sent or received by e-mail, the Internet or other means over the district computers and network becomes the property of the district and may be accessed at any time by the district for its review. In the event that a review reveals that this policy has been violated in any way or that the privilege of using the technology tools and the Internet is being abused in any way, appropriate action will be taken against the individual or individuals involved. The District may suspend or revoke a user's access to the network system upon violation of District policy and/or regulations regarding acceptable use. Termination of a student's access will be effective on the date the principal or designee revokes system privileges**.**

Violations of this policy may have disciplinary repercussions, including:

- Suspension of network, technology (school owned or BYOT), or computer privileges
- Notification to parents
- Detention or suspension from school and school-related activities
- Legal action and/or prosecution

Consequences will be based on policies established in the Student Handbook, Code of Conduct and federal and state laws. Failure to comply with this policy or directives may result in withdrawal of your access privileges, exclusion from courses of study, placement in an alternative education program, or criminal prosecution.

I have read and understand the Acceptable Use Policy and agree to abide by the provisions.

Student Name (Printed): _____ Grade: _____

Student Signature: _____ Date: _____

Parent Signature: _____