Eanes Independent School District
High School Responsible Use Guidelines for Technology

Our staff and students use technology to learn. Technology is essential to facilitate the creative problem-solving, information fluency, communication and collaboration that we see in today's global economy. While we want our students to be active contributors in our connected world, we also want them to be safe, legal, and responsible. The Responsible Use Guidelines (RUG) support our vision of responsible technology use and promote a strong sense of digital citizenship. The RUG applies to all Eanes Independent School District computer networks (including the devices made available by them), and all devices connected to those networks (whether they be student owned or otherwise).

With the ability to use technology comes responsibility. It is important you read and discuss the District Responsible Use Guidelines, ask questions if you need help understanding them, and sign the agreement form. It is your responsibility to follow the rules for appropriate use. Irresponsible system use will result in the loss of the privilege of using this educational and administrative tool. Please review the leveled-guidelines following this document, which explain in greater detail responsible use expectations for elementary, middle school and high school students in the areas of Internet Safety & Security, Digital Citizenship, and Research & Information Literacy.

Please note that the Internet is a global computer network of many types of communication and information networks. It is possible that you may run across some material you might find objectionable. While Eanes ISD will use Internet filtering technology to restrict access to such material, it is not possible to absolutely prevent such access. District provided resources are not private and may be viewed by district officials.The school district will provide you with third party accounts (such as Google Apps) that must also adhere to these Responsible Use Guidelines. Any other third party accounts that are used for educational purposes, must also adhere to these Responsible Use Guidelines. Eanes Independent School District will monitor your activity on the network and on school-issued devices.

It will be your responsibility to follow the rules for appropriate use.

RESPONSIBLE USE AND DIGITAL CITIZENSHIP	Any use described below is deemed "responsible" and consistent with the Eanes ISD Responsible Use Guidelines for Technology. The final decision regarding whether any given use of the network or technology resource is acceptable lies with the Superintendent or designee. • Use is mainly for educational purposes, but some limited personal use is permitted. (Remember that people who receive Email from you with a District address might mistakenly infer that your message represents the District's point of view). • Use furthers the educational and administrative purposes, goals, and objectives of Eanes ISD.

- Use is limited to your own individual account - you and only you should use that account. You should not share your password with others.
- Use furthers research related to education and instruction
- Use does not violate the student code of conduct or employee standards of conduct.
- Use of appropriate online names as well as use of polite and appropriate language/content on all online posts.
- Use of websites, content, and media is properly cited with respect to copyright.

UNACCEPTABLE AND IRRESPONSIBLE USE

Any of the following uses is deemed "unacceptable and irresponsible" and a violation of the Eanes ISD Responsible Use Guidelines for Technology. This list does not include all possible violations and supplements prohibited behaviors defined in the Student Code of Conduct. The final decision regarding whether any given use of the network or technology resource is acceptable lies with the Superintendent or designee.
Disciplinary action may be taken for unacceptable and irresponsible use of the network or Internet.
- Unauthorized use of copyrighted material, including violating district software licensing agreements
- Posting of videos or photos without permission of the individual or group.
- Sending, possessing, delivering, or posting electronic messages or images that are abusive, obscene, sexually oriented, harassing, threatening, intimidating, illegal, or that cause a material or substantial disruption at school or infringes on the rights of another student at school, including cyberbullying.
- Use of technology resources such as chat rooms, social sites, and games in a manner that causes disruption to the educational program
- Use of school technology resources to encourage illegal behavior or threaten school safety
- Use of personal device that conflicts with Board policy and/or the student handbook and code of conduct
- Use of any means to disable or bypass the district's Internet filtering system or other security systems
- Attempting to alter, destroy, disable or gain unauthorized access to district technology equipment, district data, the data of other users, or district network resources.
- Encrypting communications or files to avoid security review
- Posting personal information about yourself or others (such as addresses and phone numbers) other than as needed to conduct school operations

- Forgery of email messages or transmission of unsolicited junk e-mail
- Use related to commercial activities or for commercial gain
- Use that violates the student code of conduct or employee standards of conduct, or is unlawful
- Wasting school resources through the improper use of the computer and/or network systems

CONSEQUENCES FOR INAPPROPRIATE USE   One or more of the following consequences may be imposed:

- Disciplinary action, in accordance with Board policy and/or the student handbook and code of conduct (as applicable)
- Removal of personal device(s) if applicable by authorized District personnel

Internet Safety and Security

Go Places Safely and Responsibly - The internet can be a great place to discover and visit far-away places to learn new things. Staying safe online is similar to staying safe in the world. Students will choose safe, age-appropriate sites with the guidance of their teachers.

Staying Safe Online - EISD has filters in place to help steer students clear of inappropriate content; however, students may encounter some inappropriate information. Students will contact their teacher if they encounter a website that could be inappropriate.

Communicating Safely Online - Use of the internet and online collaboration is an important part of being in high school. However, there are still risks involved when engaging in online conversation. Students will recognize and report any warning signs of online predators. Students will engage in safe online relationships and not participate in inappropriate dialogue with others online. Students will identify strangers and avoid risky online behavior. Students will report any inappropriate communication or possible online predators with a trusted adult.

Security of Information - Sharing of information online can be a great way to accomplish a task or work on a project collaboratively. However, there are certain bits of information that students should not share online or with others. Students will not share any of the following:
- Passwords
- Personal information/inappropriate photos of yourself
- Personal information/inappropriate photos of others

Internet Privacy - Many websites collect information from visitors for advertising or data collection purposes. Students will:
- Recognize and analyze online privacy terms.
- Understand the how and why companies collect their information so they can make informed decisions before providing personal information to a website.
- Guard against phishing, scamming and identity theft.

Digital Citizenship

The internet is a powerful community of connected people. That connection requires levels of responsibilities to one another. Part of being a good digital citizen is using technology in a responsible, appropriate way. Digital media plays an important role in a student's life and in our society. Below are some specific areas to address with high school students when learning how to grow their digital citizenship.

Social Media & Email - Students will have access to a school email account after receiving some basic training on email etiquette. Please know that all email can be viewed by teachers, administrators, or parents. Email should be written with thought of the audience and purpose. Certain online school-approved social media sites are allowed. Students will learn about interaction, risks, and responsible use on both school-approved and other social media sites that they may encounter.   Abuse or misuse of district email or school-approved social media sites may require disciplinary action.

Commenting Responsibility - As the use of social media and other age-appropriate websites becomes available to high school students, it's important for students to understand the positive and negative aspects of their digital life. Students will recognize the importance of context in posting or viewing online images. Students will post appropriate comments in online and social communities. These comments, like anything else on the internet, have a certain amount of digital permanence and can affect reputation down the road. Students will display respect and thoughtfulness online by not posting comments that are negative, inappropriate, or personal about others or themselves.

Digital Ethics - Students will use the internet and digital tools to produce content and projects. Students will not present the work of others as their own work (otherwise known as plagiarism) Students will not intentionally delete or damage another student's digital work. Students will ask for permission prior to posting videos or photos of students or staff members online. When working on projects or any other work with online resources, students will follow copyright and creative commons laws.

Cheating - With the use of mobile devices, there may be temptation to cheat and share test or assignment information on a non-collaborative project. Students will not use technology and/or mobile devices to share confidential school content with other students.

Cyberbullying - Cyberbullying is the use of digital technologies or mobile devices to harass, threaten, embarrass or torment another student. Minors can be convicted in a court of law of being a cyberbully. This can happen both directly and indirectly. In order to avoid this students will:
- Identify strategies for dealing with cyberbullying responsibly.
- Analyze and report any offensive online behavior or interactions to a trusted adult.
- Create positive online communities rooted in trust and respect.
- Think before you send or post

- Recognize and identify factors that intensify cyberbullying, including what role they play in escalating or de-escalating online cruelty

Students will NOT:
- Publish information that is not harmful or embarrassing to others
- Facilitate in the spreading of rumors via online platforms.
- Participate in online polls, "bash" sessions, or other communities that are harmful to others.

"Sexting" or other inappropriate online interactions - Like cyberbullying, "sexting", or the transmission of inappropriate images or messages digitally, can result in conviction in a court of law. Students will understand the role of digital technologies in relationships. Students will not actively participate in the sharing of inappropriate photos and/or information of themselves or others.

Research and Information Literacy

Searching - Students will use a variety of search engines to search for information and content. Students will understand the functions of effective keywords and categories to find useful and relevant information online.

Research and Evaluation - Students will choose websites with high-quality information and when possible, use multiple sources to find their information. Students will properly cite online resources. Students will be able to identify online advertisements and spam on websites and understand the purpose behind those advertisements.