Eno River Academy: Internet Safety Policy

Approved by the ERA Board of Directors February 2023

Internet connectivity and content filtering:

Eno River Academy uses the DIT managed firewall service offered through the School Connectivity Program. The firewall is configured in accordance with security recommended practices to ensure that only ports, protocols, and services with validated business needs are allowed through the firewall.

Eno River Academy uses the MCNC web security service offered through the School Connectivity Program. The web security service provides URL filtering, to protect students from harmful online content, and advanced threat protection with full inline inspection of all inbound and outbound traffic on ports 80 and 443. Detailed service descriptions can be found at:
https://www.mcnc.org/our-community/k12/services

Acceptable Use Policy:

Eno River Academy supplies Chromebooks, laptop computers, and iPads for our students to use and share while at school. It is very important that these are treated with respect: carried with two hands, placed on flat, sturdy surfaces when in use, and plugged back into the charging carts in their numbered locations. It is also important that students use the computers appropriately for educational purposes and not personal use. Students may not access inappropriate material on the Internet, engage in any "hacking" activities or download any documents, files, programs, or visit "chat rooms" without teacher permission. There are behavior standards expected of students concerning the use of technology. All work is to be saved on students' Google Drives associated with their school-assigned email addresses or to USB flash drives. The computers are school property and if they are abused or damaged students may lose the privilege of using them or be financially responsible for necessary repairs.

Google Account:

Each student in grades 2-12 will be assigned a Google account. As such, each student will have an online account with access to Google Apps for Education including: Drive (online storage), Gmail (email), Google Docs (word processing), Slides (Presentation software), Sheets (Spreadsheet software), Sites (website software), Classroom (virtual classroom), Chrome Web Browser (World Wide Web / Internet) and many other free resources. Google is setting the standard for technology integration in education and its programs are accessible from any Internet-connected device at school and home.

The utilization of Chromebooks and Google Accounts affords us significant management and monitoring of students' usage. For email, a safeguard is set up so that 2nd through 8th Grade students may only send or receive emails from other students and teachers. For High School students, this restriction is not in place, but all emails are

monitored for objectionable content. All students' personal information is kept confidential and will not be disclosed or disseminated.

Bring Your Own Device Policy:

With the proliferation of online learning and the increasing number of students with mobile devices, Eno River Academy will allow students to bring their own device to school in order to complete academic tasks. ALL devices may only be used with individual teacher approval. Students who do bring their own devices to school are required to connect to the school's WiFi so that our protection measures may be applied. In all cases, it is the student's responsibility to gain permission before using their own device. Any unauthorized use of personal electronics will result in confiscation and require a parent/guardian to pick up the device from the principal.

Student Safety Education:

Internet safety curricula is delivered to our students by our School Counselors, P.E./Health Teacher, and/or individual classroom teachers.

In grades K-5 our Guidance Counselor uses this presentation:
https://instructional-resources.s3.amazonaws.com/PLTW_Launch/Launch_English_Cross_Unit_Resources/Digital_World_Safety_Video/index.html

And this video on online security from Project Lead the Way:
https://instructional-resources.s3.amazonaws.com/PLTW_Launch/Launch_English_Cross_Unit_Resources/Digital_World_Safety_Video/index.html

Some teachers use the following resources or adapt their own similar to these.
https://www.commonsensemedia.org/educators/erate-teachers

In grades 6-12 we use the Say Something Anonymous Reporting System and lessons (https://www.sandyhookpromise.org/our-programs/say-something/).

All High School students are instructed with this presentation:
https://docs.google.com/presentation/d/10CfzcYSqrAxeKXuzGMDRze95ITEDVrPgYliydUfMRVY/edit#slide=id.g9b7ace348e_0_21

Students borrowing school computers for off-campus use:

As we begin to allow students to borrow computers for off-campus use, specific checkout procedures will be developed along with policies dictating acceptable use, damage and replacement schedules, and other guidelines as they arise.

The same safeguards and security measures in the first section: **Internet connectivity and content filtering** are applied to school-owned devices and are in place whether they are on campus or off-campus and on a home, private, or public network.

Network Acceptable Use Policy (Taken from Eno River Academy's Comprehensive Manual)
(https://app2.boardontrack.com/attachment/publicDownload/178705?s=p8eMKf)

Section 3.22

BACKGROUND. Internet access is available to students and teachers at Eno River Academy. Our educational model requires access to the large pool of data and instructional materials available through the global network, thus its availability is not only a high priority for the school but a necessary part of the daily educational process. With access to computers and people all over the world also comes the availability of material that may not be considered to be of educational value in the context of the school setting. Eno River Academy will take precautions to restrict access to such materials. However, on a global network, it is impossible to control all materials and an industrious user may discover controversial material. We firmly believe that the valuable information and interaction available on this worldwide network far outweigh the possibility that users may procure material that is not consistent with the educational goals of the school.

RESPONSIBILITIES. 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 here so that students are aware of the responsibilities they are about to acquire. Students are expected to abide by this Network Acceptable Use Policy as well as applicable local, state, and federal laws. If an ERA student violates any of these provisions, he or she may lose any and all computer access privileges (including use for school work) for a period of time based on the severity of the violation and/or face other disciplinary consequences. Severe violations and/or violations of state or federal laws will incur more serious consequences in accordance with those policies and the law. The signatures on the Acceptable Computer Use Agreement are legally binding and indicate the parties who signed have read the terms and conditions carefully and understand their significance.

RISKS AND LIMITATION OF LIABILITY. Since ERA has no campus library or media center, the Internet serves as a powerful and essential educational tool. However, students and parents must be informed of the potential dangers that exist on the Internet, including (but not limited to) child/sexual predators, scam artists, and

hate-based materials. ERA school-based computer use policies have been developed to protect against these dangers, and student use will be monitored by school staff to enforce these policies. In addition, data that track individual student Internet activity can be made available to parents upon request. Students are hereby warned against giving out any personal information over the Internet, including physical description or photo of self, name, age, address, school attended, or any times when the student will be home alone (including after school before parents have returned from work). Students should never meet one-on-one with someone they have met on the Internet without first seeking guidance from their teacher/advisor and parent/guardian.

Unlike home-based Internet usage which may be for entertainment and other purposes, Internet usage at ERA is for educational purposes only. ERA reserves the right to block or filter Internet content that has no educational purpose, is obscene, contains pornography, or is harmful to minors. ERA makes no guarantee that the functions or services provided by or through the ERA network will be error-free or without defect. Eno River Academy will not be responsible for any damages a user may suffer including but not limited to loss of data, delays, nondeliveries, misdeliveries, or service interruptions caused by provider/user negligence, errors or omissions. ERA is not responsible for the accuracy or quality of the information obtained through or
stored in the system or network. ERA will not be responsible for financial obligations arising through the unauthorized use of the system. Use any information obtained via the Internet at your own risk.

ERA NETWORK ACCESS—TERMS AND CONDITIONS. A responsible student user of the ERA Network:

- MAY USE the Internet to research assigned classroom projects.
- MAY USE the Internet to research or develop educational materials.
- UNDERSTANDS that NONE of his or her communications and information accessible through the ERA Network is considered private or confidential.
- UNDERSTANDS that his or her Internet activity may be tracked and monitored and made available for parental review.
- UNDERSTANDS that ERA staff may be silently observing his or her workstation or device and network activity at any time, and may intervene in this activity at any time.
- AGREES that he or she will NEVER disclose his or her password to any other student.
- AGREES to NEVER disclose his or her personal information or private information about another person over the Internet either by posting or by disclosing this information to another person met on the Internet.
- UNDERSTANDS that security on any computer system serving many users is critical, and it is the responsibility of all users to help safeguard the integrity of the system. This responsibility includes the reporting of any potential security breach

such as unauthorized or prohibited use. If you feel you can identify a security problem on the network, you must notify a teacher or an administrator.

- UNDERSTANDS that if any provision of the ERA Network Acceptable Use Policy is violated, the student may not be allowed to use the ERA network and disciplinary action may be taken.

1) School Computer/Equipment Violations: If a student uses a school-owned desktop, laptop, Chromebook or other technology equipment, the student must leave the equipment exactly as he or she finds it unless given specific permission from an instructor. Prohibited changes include, but arennot limited to:
   - Installing unauthorized software on any computer or anywhere on the network.
   - Logging on as another user or allowing another individual the use of one's account or user ID.
   - Stealing, vandalizing or defacing hardware (including keyboards, monitors, and headphones).
   - Not reporting computer vandalism that one is aware of.
   - Removing or replacing hardware or cables without authorization.
   - Changing the screensaver or desktop backgrounds.
   - Moving, adding, deleting, or changing icons on the desktop, including printer icons.
   - Setting themes or sounds, changing the screen resolution or tampering with operational settings including the Start menu.
2) Usage Violations: Use of the ERA network must be in support of education and research and consistent with the educational objectives of Eno River Academy. The student is responsible, at all times, for its proper use. Improper use of the ERA network is prohibited. Uses of the ERA network that are prohibited include, but are not limited to:
   - Use of ERA technologies in support of any illegal purposes.
   - Intentionally uploading, creating, or spreading computer viruses or worms.
   - Attempting to gain unauthorized access to the ERA network, or any other network, or to any secure data is considered hacking activity and thus is prohibited. Hacking activity includes students attempting to logon to the network/Internet as a faculty member or an administrator, including accessing a student or staff account that has been left open by mistake.
   - Possessing and/or using or attempting to use hacking tools, including keystroke loggers and password/encryption tools.
   - Not reporting network security violations or potential violations that you are aware of. If you become aware of a problem, do not demonstrate the problem to other users.
   - Downloading and storing files on the network without authorization. Logging on as another user or allowing another individual the use of one's account or userID. When logged in properly, students have authority to download and store materials that do not violate other conditions of the agreement.

• Providing access to the ERA network to unauthorized individuals via one's own account, another's account, or otherwise.

• Using profanity, obscenity or language that is considered offensive or threatening to persons of a particular race, gender, religion, sexual orientation, or to persons with disabilities. This includes retrieving, viewing, producing, posting, or sending (or attempting to post or send) material that is profane, obscene, lewd, sexually explicit or suggestive or pornographic in purpose, advocates or engages in illegal acts, threats, hate or violence, or potentially disrupts, causes damage, threatens or endangers students or staff. So-called "sexting" may result in criminal prosecution and registration as a sex offender.

• Spamming: Distributing mass e-mail messages and chain letters or sending e-mail to school address lists or other large numbers of people or a large volume of messages to one or more individuals for the purpose of causing annoyance.

• Posting personal or private information about yourself or other people on the Internet. Violating any aspect of a student's, or staff member's right to privacy by disclosing confidential information including, but not limited to, a student's grades or test scores.

• Posting, sending, or disclosing over the Internet information that insults, defames, or harasses.

• "Re-posting" or forwarding personal communications without the author's prior consent.

• Chat rooms and instant messaging are off-limits during school hours except for classroom purposes. Arranging or agreeing to meet with a person you have met online without specific advance permission from a parent or teacher is prohibited.

• Using ERA technology to copy commercial software in violation of state, federal, or international copyright laws.

• Using the ERA network for financial gain or for the transaction of any business, commercial or lobbying activities.

• Using technology to cheat; to misrepresent another's work as one's own or to pass one's work on to another for the purpose of cheating.

• Plagiarizing (claiming another person's writings as your own) any information gained on or through the network or from the Internet. (This includes the downloading of reports or term papers purchased on the Internet and passing them off as one's own).

3) Conduct Violations: The use of the computer/device is a privilege, not a right, and inappropriate use will result in disciplinary action. The school administrators will deem what is inappropriate use, based on the explicit and implicit guidelines in the Network Acceptable Use Policy. You are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

• Do not be rude or abusive in your messages to others.

• Use only appropriate language. Do not swear or use vulgarities or any other inappropriate or offensive language.

• If you find a student or staff account that is left open or logged in, you must close the account immediately and notify a staff member. Accounts may contain personal or restricted information.
• Using technology for off-task activities during class (playing games, videos, music, or visiting websites not instructionally related) is prohibited without permission from your teacher.
• You must report to a staff member any unsolicited or inappropriate web site that pops up on your screen without your consent.
• It is your responsibility to keep your password confidential. IF YOUR PASSWORD IS COMPROMISED, YOU MUST CHANGE IT IMMEDIATELY! If you forget your password, see your teacher or advisor, who will help you create a new password. Choose a password you can easily remember.