**Acceptable Use Policy**

All students are expected to conduct their online activities in an ethical and legal fashion. **The use of these resources is a privilege, not a right**. Misuse of these resources may result in the suspension or loss of these privileges, as well as any disciplinary, legal, or other action deemed necessary. Examples of inappropriate or unacceptable use(s) of these resources include, but are not limited to, those uses that violate the law, the Acceptable Use Policy, this Handbook, and any behaviors that would disrupt the educational environment or hamper the integrity or security of the school network. **Some unacceptable practices include, but are not limited to:**

- The use of Instant Messaging or screen-sharing programs with other students during school hours is prohibited.
- Transmission of any material in violation of any U.S. or state law, including but not limited to: copyrighted material without the written permission of the author or creator; threatening, harassing, pornographic, or obscene material; or material protected by trade secret is prohibited.
- As with all forms of communications, e-mail or other network resources may not be used in a manner that is disruptive to the work or educational environment. The display or transmission of messages, images, cartoons or the transmission or use of e-mail or other Chromebook messages that are sexually explicit constitute harassment, which is prohibited by the district.
- The use for personal financial, political, or commercial gain, product advertisement, or the sending of unsolicited junk mail or chain letters is prohibited.
- The forgery, reading, deleting, copying, or modifying of electronic mail messages of other users is prohibited.
- The creation, propagation, and/or use of viruses or other malicious software is prohibited.
- Deleting, examining, copying, or modifying files and/or data belonging to other users is prohibited.
- Unauthorized copying/installation of software programs is prohibited.
- Intentional destruction, deletion, or disablement of installed software is prohibited.
- Vandalism is prohibited. This includes, but is not limited to, any attempt to harm or destroy the data of another user, the network/Internet, or any networks or sites connected to the network/Internet. Attempts to breach security policies, codes, and/or passwords are considered a form of vandalism.
- Destruction of hardware or software or attempts to exceed or modify the parameters of the system is prohibited.
- All passwords must be safeguarded. These include, but are not limited to, network, internet, and email accounts. Your accounts are your responsibility. All violations that can be traced to an individual account name will be treated as the sole responsibility of the account owner. Users of the network should never use a computer that has been logged in to by another user or log into a computer designated as a teacher computer/workstation.

Access to school e-mail and similar electronic communication systems is a privilege, and certain responsibilities accompany that privilege. Students are expected to demonstrate the same level of an ethical and professional manner as is required in face-to-face or written communications. All

users are required to maintain and safeguard password-protected access to both personal and confidential district files and folders.

Attempts to access another person’s e-mail or similar electronic communications or to use another's name, e-mail, or device to send an e-mail or similar electronic communications are prohibited and may be subject to disciplinary action. Anonymous or forged messages may be treated as violations of this policy. Nothing in this policy shall prohibit the district from intercepting and stopping e-mail messages that have the capacity to overload the district resources. All users must understand that the district does not guarantee the privacy or confidentiality of electronic documents and any messages that are confidential as a matter of law should not be communicated over e-mail.

The district reserves the right to access e-mail to retrieve information and records, to engage in routine device maintenance and housekeeping, to carry out internal investigations, to check Internet access history, or to disclose messages, data, or files to law enforcement authorities. **Any information contained on any technology that is transmitted through or purchased by the ECASD is considered the property of the district**. Files stored or transmitted on district equipment, cloud services, or the network are property of the district and are subject to review and monitoring. **The district reserves the right to confiscate the property at any time**.

This agreement applies to all devices connected to the district network or Internet. Any attempt to violate the provisions of this agreement could result in revocation of the user's privileges or other disciplinary action, regardless of the success or failure of the attempt. In addition, school disciplinary action, and/or appropriate legal action may be taken. The decision of the Technology Department and building administrators regarding inappropriate use of the technology or telecommunication resources are final. Monetary remuneration may be sought for damage necessitating repair, loss, or replacement of equipment and/or services.