

**Administrative Procedure - Acceptable Use of the District's Electronic Network and Instructional Technology**

**Definitions**

**Electronic Network** - The District's electronic network includes, but is not limited to, its cloud storage, servers, routers, switches, connections, hardware, and all connected devices, regardless of whether they are owned by the District, including computers, laptops, Chromebooks, tablets, cell phones, copiers, and printers.

**Instructional Technology** - All computers, laptops, Chromebooks, tablets, cell phones, email, educational technologies, online applications or services, mobile applications, network files, computer files, or accounts designed, marketed, primarily used for, or provided or made available by the District to students or staff for K-12 school purposes.

**Terms and Conditions**

All use of the District's electronic network and instructional technology shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. This procedure does not attempt to state all required or prohibited behavior by users. However, some specific examples are provided. **The failure of any user to follow this procedure may result in the loss of privileges, disciplinary action, and/or legal action.**

1. **Use is a Privilege** - Use of the District's electronic network and instructional technology is a privilege, not a right. Inappropriate use of these resources may result in loss of privileges, disciplinary action, and/or referral to legal authorities by school administrators. Access to the District's electronic network or instructional technology may be limited, suspended, or revoked at any time.
2. **Acceptable Use** - All use of the District's electronic network or instructional technology must be: (1) in support of education and/or research, and consistent with the District's educational objectives, or (2) for a legitimate school business purpose. Staff members shall supervise students while students are using the District's electronic network and instructional technology to ensure students abide by the Terms and Conditions for access contained in this procedure.
3. **Unacceptable Use** - The user is responsible for his or her actions and activities involving the District's electronic network and instructional technology. Some examples of unacceptable uses are:
  - a. Using the electronic network or instructional technology for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any State or federal law;
  - b. Recording an audio or video conference (e.g. Google Meet, Webex, Zoom) without disclosing the conference is being recorded and without the permission of a staff member;
  - c. Unauthorized downloading of software, regardless of whether it is copyrighted or de-licensed;
  - d. Downloading of copyrighted material for other than personal use;
  - e. Using the electronic network or instructional technology for private financial or commercial gain;
  - f. Wastefully using resources, such as file space;
  - g. Hacking or gaining unauthorized access to files, resources, or entities;

- h. Invading the privacy of individuals, that includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature including a photograph;
  - i. Using another user's account or password;
  - j. Posting material authored or created by another without his/her consent;
  - k. Posting anonymous messages;
  - l. Using the electronic network or instructional technology for commercial or private advertising;
  - m. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; and
  - n. Using the electronic network or instructional technology while access privileges are suspended or revoked.
4. **Network Etiquette** - Each user is expected to abide by the generally accepted rules of user etiquette. These include, but are not limited to, the following:
- a. Be polite. Do not harass, attack, or become abusive in messages to others. Do not send or display offensive messages or pictures.
  - b. Use appropriate language. Do not swear, use obscene, vulgar, or any other inappropriate language.
  - c. Do not reveal personal or confidential information, including personally identifiable information contained in student records or personal addresses, telephone numbers, or email addresses of students or colleagues.
  - d. Recognize that communication is not private. People who operate the District's electronic network have access to all communication sent via email or District provided apps. Messages relating to or in support of illegal activities may be reported to the authorities.
  - e. Do not use the District's electronic network in any way that would disrupt its use by other users.
5. **Filtering, Monitoring, and Review** - The District filters Internet content on the District's electronic network and instructional technology in order to comply with local, state, and federal laws and to remove access to websites and Internet servers that contain visual depictions that are: (1) obscene, (2) pornographic, or (3) have been deemed to contain harmful or inappropriate content, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee. Report any errors found regarding filtered or unfiltered sites immediately to an administrator or the Technology Department. Information stored, transmitted, or communicated on the District's electronic network or instructional technology is not to be considered private or permanent. The District retains the right to monitor the District's electronic network and instructional technology use without warning or notice and to remove data or files found on the electronic network or instructional technology that violate this procedure or that are not in direct support of an educational purpose or business. The District further retains the right to maintain and review back-up copies of the District's electronic network, instructional technology, electronic systems, files, data, apps, communications, and email. Information gained through monitoring or review may be used as evidence in any disciplinary or legal action.
6. **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 may

suffer while using the District's electronic network or instructional technology. These damages may include, but are not limited to, loss of data as a result of delays, non-deliveries, mis-deliveries, or service interruptions caused by the system or by employee error or omission. Use of any information obtained via the information system is at the user's own risk. The District specifically denies any responsibility for the accuracy of information obtained through electronic information resources.

7. **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 violation of this procedure.
8. **Security** - Electronic network security is a high priority. If the user can identify a security problem on the District's electronic network, the user must notify the system administrator or building administrator. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account without written permission from that individual. Attempts to log-on to the District's electronic network as a system administrator will result in revocation of user privileges. Any user identified as a security risk may be denied access to the electronic network.
9. **Vandalism** - Vandalism is defined as any malicious attempt to harm or destroy property of the user, another user, or of any other agencies or networks that are connected to the District's electronic network as well as the Internet. Vandalism also includes, but is not limited to, overloading of data on the server as well as the uploading, downloading or creation of computer viruses in an intentional manner. Vandalism is considered a violation of this procedure and as such is subject to loss of privileges, disciplinary action, or legal action as deemed appropriate by the administration.
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 websites or file servers without explicit written permission.
  - a. For each re-publication (on a website 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 provide library media specialists with email or hard copy permissions 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 website 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. **Student Email** - Email provided to students and staff of the District is primarily for internal educational communications. Student email addresses should not be made available to the public unless deemed appropriate by the administration. Student personal use of District provided email resources is prohibited. Any use should be in the scope of the educational

curriculum and teacher expectations of utilizing the tool for instructional purposes. Student to student, student to teacher, student to administrator email correspondence should follow proper etiquette guidelines listed in Section 4 of this procedure.

- a. 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 email account is strictly prohibited.
- b. Each person should use the same degree of care in drafting an email message as would be put into a written memorandum or document. Nothing should be transmitted in an email message that would be inappropriate in a letter or memorandum.
- c. Electronic messages transmitted via the School District's Internet gateway carry with them an identification of the user's Internet domain. This domain is a registered 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 the School District. Users will be held personally responsible for the content of any and all email messages transmitted to external recipients.
- d. 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.
- e. Use of the School District's email system constitutes consent to these regulations.

**13. Receipt and Agreement** - Acknowledgement by parents and students of receipt and agreement to this procedure during registration is required before access to the District's Network will be granted. Staff will acknowledge receipt and agreement to this procedure on an annual basis.