Access to Electronic Resources and Technology and Acceptable Use Policy

Section A - Introduction

To ensure that the use of the District's electronic resources and technology by its employees, contractors, agents, volunteers, and students is appropriate and consistent with the goals and policies of the District, and to protect the welfare of both employees and students, the Board of Education has established this Acceptable Use Policy (AUP).

Section B - Definitions

District Business - Any work conducted as an employee, contractor, or agent of the District, whether for educational, extra-curricular, or other business or operational purposes of the District. District business includes, but is not limited to work that relates to education, instruction, student and employee relations and discipline, extra-curricular activities, professional activities, and other District operations.

Electronic Resources - These resources include, but are not limited to, the District's electronic networks and information systems, such as the internet, Wi-Fi, electronic data networks, and infrastructure for oral, visual, and written electronic communication, including electronic mail, text messaging, instant messaging, and chat programs. These resources also include technology owned or licensed by the District and provided by the District for use by its employees, contractors, agents, volunteers, and students. If an employee, contractor, agent, volunteer, or student accesses the District's electronic resources on-premise, or remotely, including internet service or Wi-Fi, with a personal technology device, that access is also considered a use of Technology and Network Resources covered by this AUP.

System Administrator - The Chief School Business Official or designee.

Technology - Technology includes, without limitation, desktop computers, laptop computers, tablet computers, cell phones and smartphones, software created by or licensed by the school district, databases utilized or maintained by the school district, text messaging services, instant messaging services, and other technology, as well as any webpages or social media profiles, such as internet forums, blogs, video logs, wikis, social networks and social media pages, podcasts, photograph, and video sharing programs, rating websites, music-sharing websites, and crowdsourcing.

User - A user of the District's electronic resources is any person who uses the District's electronic resources, with or without District authorization, and may include, but is not limited to, employees, contractors, agents, volunteers, parents, and students of the District.

Section C - Purpose of Electronic Resources and Technology

Electronic Resources and Technology:

- Are for the use of employees, contractors, agents, volunteers, students, and visitors;
- Are intended to provide authorized users with appropriate equipment and software to accomplish their District-authorized missions and to provide access to electronic resources;
- Are intended for academic and administrative purposes only, as more fully described in Section F; and
- Are not intended to be used for non-academic or non-administrative functions or for personal or recreational use, which include, but shall not be limited to, illegal, commercial, political, religious, or entertainment purposes, as more fully described in Section G.

Section D - Privileges

Using the District's Electronic Resources and Technology is a privilege, not a right, and inappropriate use may result in canceling those privileges, disciplinary action, and appropriate legal action. The Superintendent or designee in the case of an employee, or the Principal or designee in the case of a student, will make all decisions regarding whether or not a user has violated these procedures and may deny, revoke, or suspend access at any time.

Section E - Indemnification

By using the District's Electronic Resources and Technology, the user agrees to indemnify the District, including the Board of Education and its members, for any losses, costs, or damages, including reasonable attorney fees, incurred by the District, including the Board of Education and its members, relating to, or arising out of, any violation of this policy.

Section F - Acceptable Uses of Electronic Resources and Technology

Acceptable uses of the District's Electronic Resources and Technology include, but are not limited to, the following:

1. Curricular, instructional, co-curricular, and school-related extra-curricular activities or uses in support of such activities.
2. Research consistent with the goals and purposes of the District.
3. Communication among students, faculty, staff, and the local, regional, state, national, and global communities for academic or administrative purposes.
4. Development and implementation of the curriculum.
5. Professional development of staff members.
6. Administrative or managerial record keeping, data access, or research.

Section G - Unacceptable Uses of Electronic Resources and Technology

The user is responsible for his or her actions and activities involving Electronic Resources and Technology. Unacceptable uses of technology and network resources include, but are not limited to, the following:

1. Participating in, promoting, or facilitating any activity that violates Federal, state, or local laws or regulations;
2. Using Electronic Resources and Technology to engage in conduct prohibited by Board Policy or the Parent and Student Handbook;
3. Interfering with, damaging, modifying, gaining access to in an unauthorized manner, or disrupting computer or network users, services, data, or equipment.
4. Conducting District business using technology that has not been authorized for such business by the System Administrator.
5. Participating in the acquisition, creation, or distribution of materials that are libelous, obscene, pornographic, promote the use of violence, contain personally embarrassing or private information unrelated to any proper educational or public purpose, contain defamatory or untrue statements that may damage the reputation of any student or staff member, or contain abusive, harassing, or prejudicial content.
6. Participating in the acquisition, creation, or distribution of advertising, computer "worms" or "viruses," "chain letters," "spam," or other messages/files that could cause congestion, interference, or failure of the system or any computing equipment, whether attached to the District's system or otherwise.

7. Making unauthorized entry to any computer, network, file, database, or communications device regardless of who may own, operate, or supervise the same and whether or not a change of data or software occurs.
8. Altering, damaging, or destroying any cabling, hardware, or software or making unauthorized changes to District data.
9. Accessing, using, possessing, distributing, or disseminating unauthorized or illegally obtained hardware, software, or data.
10. Engaging in any activity that does not conform to the intended purposes of the network, including, but not limited to, illegal, commercial, political, religious, recreational, or entertainment purposes.
11. Using technology and network resources or data for academic dishonesty.
12. Using another user's account or password.
13. Disclosing any network or account password (including your own) to any other person unless requested by the System Administrator.
14. Misrepresenting the user's identity or the identity of others.
15. Using the electronic networks while access privileges are suspended or revoked.

Section H - Compliance with Internet Safety

Each District-owned computer with internet access or a personal computer that is accessing the school district's network has a filtering device that blocks entry to visual depictions that are (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee. Other sites that may be filtered include non-educational sites that seriously degrade the performance of the network or pose network intrusion risks and sites that will result in unplanned or unauthorized costs to the District.

The System Administrator and Principal or designee shall monitor student Internet access.

Section I - No Expectation of Privacy

Users who use the District's Electronic Resources and Technology have no expectation of privacy concerning the use of the District's Electronic Resources and Technology, including access to the District's internet or Wi-Fi using personal technology or concerning any material created, transmitted, accessed, or stored via the District's Electronic Resources and Technology. This lack of expectation of privacy includes material produced, transmitted, accessed, or stored for personal use, including incidental personal use, on or through the District's Electronic Resources and Technology. The District reserves the right to monitor users' activities on District Electronic Resources and Technology at any time for any reason without prior notification; to access, review, copy, store, and delete any electronic information accessed or stored therein; and to disclose such information to others as it deems necessary and as required by law. Users should be aware that information may remain on the District's Electronic Resources and Technology even after the User has deleted it.

Section J - No Warranties

The District makes no warranties of any kind, whether expressed or implied, for its Electronic Resources and Technology. The District is not responsible for any damages a user experiences. This includes data loss resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by negligence or the user's errors or omissions. Use of any information obtained via the internet is at the user's own risk.

The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Section K - Security

Security is a high priority. If the user can identify or suspects a security problem when using any Electronic Resources or Technology, the user must promptly notify the System Administrator. Such user shall not demonstrate the problem to other users. Users must keep user account(s) and password(s) confidential. Users may not use another individual's account without written permission from that individual. Attempts to log on to the network as a System Administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied network access.

Section L - Vandalism

Vandalism, will result in the cancellation of privileges and other disciplinary actions. Vandalism is defined as any malicious attempt to harm or destroy the data of another user, the internet, or any other network. This includes but is not limited to, the uploading or creation of malware, such as viruses and spyware.

Section M - Disciplinary Action

1. Any student determined by the Principal or designee to violate this policy may have his/her Electronic Resources and Technology access suspended or canceled or be prohibited from possessing self-provided technology devices in school buildings, on school grounds, and at or about school-sponsored activities at any location. In addition, the student may be considered guilty of gross disobedience or misconduct and subject to additional disciplinary action by the administration and Board of Education. Such action may include but is not limited to, suspension and expulsion from school.
2. Any employee, contractor, agent, or volunteer determined by the Superintendent or designee to have violated this policy may have his or her Electronic Resources and Technology access suspended or canceled. In addition, the employee, contractor, agent, or volunteer may be subject to additional disciplinary action by the administration and Board of Education and may be required to provide user credentials for any user-based technologies or networks. Action by the Board of Education may include but is not limited to, suspension with or without pay and termination of employment.
3. Cases involving suspected or alleged criminal acts will be referred to appropriate law enforcement agencies.

Section N - Termination of Authorized Use

The Board of Education recognizes the need for secure computing and networking facilities and authorizes the administration to terminate network/computer access when said access is no longer needed. Reasons for terminating the authorized use by an individual--student or other user--may include, but shall not be limited to the following:

1. A student is no longer enrolled in the District due to graduation, transfer to another school, dropping out of school, expulsion, death, or other reasons.
2. A student attends an educational facility outside the District full-time but is still enrolled as a student.
3. A staff member is no longer employed at or is on leave from the District due to leave of absence, retirement, resignation, termination, death, etc.

4. Disciplinary reasons or violation of this policy.
5. Such other cause as the Superintendent or designee determines in the exercise of reasonable discretion is necessary to secure the network operations, functionality, and compliance with Board Policy pending further action in any disciplinary matter and pending finalization of such disciplinary determination or completion of any investigation.
6. Written revocation of consent by the student's parent or guardian.

Section O - User Training

Users of Electronic Resources and Technology shall successfully complete an appropriate training program as the District prescribes before being allowed to access the system. Depending upon the user's needs, training may include, but shall not be limited to, login and logout procedures, access and use of various computer programs and network services, and instruction regarding the security of accounts and passwords, copyright laws, computer ethics, and network etiquette. Users are responsible for reporting any violations of this policy to an administrator.

Section P - Dissemination to Employees and Students

1. All employees will be given a copy of the Board Policy for signature. New employees will be given a copy of the Board Policy to sign when signing their employment contracts.
2. Excerpts of this policy will be included in the Parent and Student Handbook.

Revised: September 5, 1995
Revised: May 29, 2001
Revised: July 28, 2003
Revised: September 12, 2005
Revised: August 10, 2009
Revised: August 8, 2011
Revised: October 28, 2024