Humboldt County School District: Acceptable Use Policy and Guidelines for Digital Information, Communication, and Technology Resources

School Year 2025-2026

The Humboldt County School District (the District) is committed to providing a rich learning and working environment supported by modern technology. This document outlines the **Acceptable Use Policy (AUP)** and provides **Guidelines for Implementation** regarding the use of our digital information, communication, and technology resources.

Scope of Policy

The Humboldt County School District provides access to technology devices, the Internet, and data systems to all employees and students for essential educational and District business purposes. This Acceptable Use Policy (AUP) governs all electronic activity of individuals using and accessing the District's technology, Internet, and data systems, regardless of the user's physical location.

This policy is adopted in compliance with the Children's Internet Protection Act (CIPA) and relevant sections of Nevada law, including NRS 388.134, NRS 388.271, 388.272, NRS 603A and student data privacy provisions under SB 463 and SB 403. The policy is reviewed annually, published on the District's website, and revised as state and federal law evolve.

All vendors handling student educational data must contractually agree to comply with Nevada's student data privacy laws (SB 403 outlines disclosure control and SB 463 outlines condition of third-party access) and district security practices, which strictly prohibit commercial profiling, targeted advertising, or unauthorized dissemination of personally identifiable student information.

Parents or guardians have the right to inspect and request corrections to their child's educational records and must provide written consent for disclosures beyond direct educational use, unless permitted by law.

The District provides annual staff training on acceptable use, data privacy, online safety, and breach response according to Nevada Department of Education guidelines.

Guiding Principles

Our approach to technology integration within the Humboldt County School District is founded on the following principles:

- **Enhancing Learning and Operations:** Online tools, including social media, should be strategically utilized across our classrooms, schools, and central offices to foster community engagement, enhance staff and student learning experiences, and improve core operational efficiency.
- **Protecting Data Privacy:** The Humboldt County School District has a legal and ethical obligation to protect the personal data and privacy of our students, families, and staff.

- **Empowering Local Implementation:** The District will provide a foundational set of policies and structures, allowing individual schools the flexibility to implement technology in ways that best meet the unique needs of their students and communities.
- **Ensuring Awareness and Responsibility:** All students, families, and staff members must be fully aware of their rights and responsibilities as outlined in this Acceptable Use Policy and relevant government regulations.
- **Upholding Rights:** Nothing in this policy shall be interpreted to limit an individual's constitutional rights to freedom of speech or expression or to restrict an employee's ability to engage in concerted, protected activity with fellow employees regarding the terms and conditions of their employment.

Compliance Requirement for Employees

This Acceptable Use Policy is reviewed annually by the Superintendent or his/her designee, and is issued via official District communication channels (e.g., Superintendent's Memo). All technology users are required to verify annually that they have read and will abide by this Acceptable Use Policy. A copy of any updates to the policy will be submitted to the Nevada Department of Education within 30 days of approval.

Student AUP & Contract

Copies of this Acceptable Use Policy and the accompanying Student Contract for Internet Use are included in the **Humboldt County School District Guide for Families & Students**, which is distributed to all students at the beginning of each school year. The Student Contract for Internet Use must be completed and signed by all students and their parent/guardian after a thorough review of this AUP together. The signed contract must be returned to the school before the student may begin using the Internet on District resources.

Consequences of Policy Breach

The use of all Humboldt County School District technology resources is a **privilege, not a right**. By using District Internet systems and devices, the user agrees to adhere to all District regulations, policies, and guidelines. Students and staff are strongly encouraged to report any misuse or breach of protocols to appropriate personnel, including building administrators, direct supervisors, and the District's Technology Services Department. Abuse of these privileges may result in one or more of the following consequences:

- Limitations of use or access privileges by placement in a highly restricted user group.
    - For students served through Special Education or a 504 plan of assistance, restrictions will be implemented through the students IEP/504 plan.
- Financial responsibility for damages or necessary repairs.

- Discipline under applicable District policies, up to and including termination of employment, subject to any collective bargaining obligations.
- Liability under applicable civil or criminal laws.

Key Definitions

- **Nevada Public Records Law under NRS 239:** A state and federal law that allows for the release of government documents at the request of an individual. A FOIA request can be made to the Humboldt County School District for electronic documents/communications stored or transmitted through District systems, unless that information is protected from disclosure by law or could be detrimental to governmental or personal interests.
- **Family Educational Rights and Privacy Act (FERPA):** A federal law that protects the privacy, accuracy, and release of information for students and families within the Humboldt County School District. Personal information stored or transmitted by agents of the District must abide by FERPA laws. The District is required to protect the integrity and security of student and family information. Families may opt out of directory information disclosure by submitting a written request.
- **Children's Internet Protection Act (CIPA):** Requires schools that receive federal funding through the E-Rate program to protect students from content deemed harmful or inappropriate. The Humboldt County School District is required to filter internet access for inappropriate content, monitor the internet usage of minors, and provide education to students and staff on safe and appropriate online behavior.
- **Data Breach:** When an unauthorized access occurs that compromises confidentiality or integrity of protected data, the district shall notify affected individuals as soon as practicable, but no later than 30 days after discovery as required by NRS 603A.

Communication & Social Media

Employees and students are provided with District email accounts and online tools to enhance the efficiency and effectiveness of communication, both within the organization and with the broader community. All communication should maintain a professional standard consistent with other forms of official correspondence. When using online tools, members of the Humboldt County School District community must exercise appropriate behavior, especially:

a) When acting as a representative or employee of the Humboldt County School District. b) When the communication impacts or is likely to impact the classroom or working environment within the Humboldt County School District.

All communication sent by an employee using District property or regarding District business could be subjected to public access requests submitted through the Freedom of Information Act (FOIA). Users need to be aware that data and other material/files maintained on the school district's systems may be subject to review, disclosure, or discovery. Use of personal email accounts and communication tools to

conduct District business is strongly discouraged and may lead to an individual's personal account being subject to FOIA inquiries. The Humboldt County School District will cooperate fully with local, state, and federal authorities in any investigation concerning or related to any illegal activities or activities not in compliance with District policies or government regulations.

Guidelines for Online Communication:

- Communication with students should never include content of a personal nature.
- When communicating with parents/guardians of students, employees should use email addresses and phone numbers listed in the Student Information System (SIS) unless steps have been taken to verify that the communication is occurring with a parent/guardian who has educational rights for the student.
- When communicating with a parent/guardian, refrain from discussing any non-related students when possible.
- Employees who use internal or external social media (e.g., blogs, Twitter, etc.) are expected to refrain from discussing confidential information and/or discussing specific students. Information that can be traced back to a specific student or could allow a student to be publicly identified should not be posted on any social media sites.
- When using social media, employees are expected to refrain from posting any negative comments online about students, or other staff.
- Employees are required to notify their principal/supervisor before setting up an online site to facilitate student learning. Employees are encouraged to monitor/moderate online communication to the best of their abilities.
- Employees are advised not to add any current or former students or parents as 'friends' or contacts on personal social media unless the site is specifically set up to support classroom instruction or school business, and approved by a supervisor.
- Employees may communicate with District graduates (18 years or older) on social media but should always maintain professionalism and caution when communicating online.
- Employees are advised not to add parents/guardians of students as 'friends' or contacts on personal social media to maintain professionalism and to avoid any appearance of conflict of interest.
- Avoid responding to spam or phishing attempts that require a user to click on any links or to provide any account information. **Note: The Humboldt County School District will never ask for a user's account password for any purpose, and users are advised to report any suspicious requests for account information directly to the District's Technology Services Help Desk.**

Solicitation

Web announcements and online communication promoting a business are prohibited by the Humboldt County School District's Solicitation Policy. Exceptions may be made by the Superintendent's Office if benefits are judged sufficient to merit such an exception.

Use of Copyrighted Materials

Violations of copyright law that occur while using the District network or other resources are prohibited and have the potential to create liability for the District as well as for the individual. Humboldt County School District staff and students must comply with all regulations on copyright and plagiarism that govern the use of material accessed through the District network.

Users will refrain from using materials obtained online without requesting permission from the owner if the use of the material has the potential of being considered copyright infringement. The District will cooperate with copyright protection agencies investigating copyright infringement by users of the computer systems and network of the Humboldt County School District.

Network Usage

Network access and bandwidth are provided to schools for academic and operational services. The Humboldt County School District reserves the right to prioritize network bandwidth and limit certain network activities that are negatively impacting academic and operational services. Users are prohibited from using the District network to access content that is inappropriate or illegal, including but not limited to content that is pornographic, obscene, illegal, or promotes violence.

Network Filtering & Monitoring

As required by the Children's Internet Protection Act (CIPA), the Humboldt County School District is required to protect students from online threats, block access to inappropriate content, and monitor Internet use by minors on school networks. The District's Technology Department is responsible for managing the Internet filter and will work with the District community to ensure the filter meets the academic and operational needs of each school while protecting minors from inappropriate content.

By authorizing use of technology resources, the District does not relinquish control over materials on the systems or contained in files on the systems. **There is no expectation of privacy related to information stored or transmitted over the Humboldt County School District network or in District systems.** The District reserves the right to access, review, copy, store, or delete any files (unless other legal restrictions apply) stored on District computers and all employee and student communication using the District network. Electronic messages and files stored on District computers or transmitted using District systems may be treated like any other school property. District administrators and network personnel may review files and messages to maintain system integrity and, if necessary, to ensure that users are acting responsibly. The District may choose to deploy location tracking software on devices for the sole purpose of locating devices identified as lost or stolen. The District shall limit use to loss/theft recovery only; tracking must not be used for employee/student surveillance.

Personal Use

The Humboldt County School District recognizes that users may utilize District email, devices, and network bandwidth for limited personal use; however, personal use should not interfere with or impede District business and/or cause additional financial burden on the District. Excessive use or abuse of these privileges can be deemed in violation of this Acceptable Use Policy. Personal use shall not include transmission of sensitive data or use of non-approved third-party systems.

Network Security

The District's Wide Area Network (WAN) infrastructure, as well as building-based Local Area Networks (LANs), are implemented with performance planning and appropriate security measures in mind. Modifications to an individual building network infrastructure and/or use will affect LAN performance and will reduce the efficiency of the WAN. For this reason, any additional network electronics including, but not limited to, switches, routers, and wireless access points must be approved, purchased, installed, and configured solely by the District's Technology Department to ensure the safety and efficiency of the network. Users are prohibited from altering or bypassing security measures on electronic devices, network equipment, and other software/online security measures without the written consent of the Technology Director. Any detected circumvention may result in investigation under NRS 205.4765.

Data & Systems

Access to view, edit, or share personal data on students and employees maintained by the District's central offices, individual schools, or by persons acting for the District must abide by local, state, and federal regulations, including the Family Educational Rights and Privacy Act (FERPA). Student and staff information and data may only be shared with individuals deemed eligible to have access by the person(s) responsible for oversight of that data. Outside parties and/or non-District individuals requesting protected data must receive approval from the District Administration (e.g., Legal Counsel or Superintendent's Office) and have a non-disclosure agreement with the District. Individuals requesting ongoing access to data through District systems are required to have a designated District administrator who will act as a "sponsor" to ensure the safety and integrity of the data.

Electronic Transmission of Data

When educational records or private data are transmitted or shared electronically, staff are expected to protect the privacy of the data by password-protecting the record/file and only using District-approved systems to transmit data. All transmissions of educational records must use encryption protocols approved by the District's Technology Department. Staff are also expected to ensure records are sent only to individuals with a legitimate right to said records and must take all reasonable measures to ensure that only the intended recipients are able to access the data.

Passwords

Users are required to adhere to password requirements set forth by the Humboldt County School District when logging into school computers, networks, and online systems. Users are not authorized to share their password and must use extra caution to avoid email scams that request passwords or other personal information.

Media & Storage

All local media (e.g., USB devices, external hard drives, CDs, flash drives) containing sensitive data must be securely protected with a password and/or encrypted to ensure the safety of the data contained. Use of cloud-storage services for storage or transmission of files containing sensitive information must be approved by the District Administration and the Technology Department. Cloud platforms must meet minimum SOC 2 or ISO 27001 certification standards. Users are encouraged to use District-approved data/information systems for the storage and transmission of sensitive data whenever possible and avoid storage on local hardware that cannot be adequately secured.

Electronic Devices

The Humboldt County School District defines electronic devices as, but not limited to, the following:

- Laptop and desktop computers, including similar devices
- Tablets
- Wireless email and text-messaging devices (e.g., e-readers, media players with connectivity)
- Smartphones
- Donated devices accepted by the District

Device Support

The District provides basic installation, synchronization, and software support for District-issued electronic devices. Devices must be connected to the District network on a regular basis to receive up-to-date software and antivirus updates and for inventory purposes. Password protection is required on all District-issued electronic devices to prevent unauthorized use in the event of loss or theft. Users are responsible for making periodic backups of data files stored locally on their devices. Backups must be stored on District-approved platforms; users should refrain from storing sensitive date locally when avoidable.

Loss/Theft

Users must take reasonable measures to prevent a District-issued device from being lost or stolen. In the event an electronic device is lost or stolen, the user is required to **immediately notify appropriate school staff and/or their direct supervisor, local authorities (if applicable), and the District's Technology Help Desk.** The District will take all reasonable measures to recover the lost property and to ensure the security of any information contained on the device. Users may be held financially responsible in cases of negligence. If unrecoverable, the District may initiate remote data deletion in accordance with its policies and procedures.

Return of Electronic Devices

All technology purchased or donated to the Humboldt County School District is considered District property. Any and all equipment assigned to employees or students must be returned prior to leaving their position or school. All equipment containing sensitive information and data must be returned directly to the Technology Services Department before it can be redeployed.

Personal Electronic Devices

The use of personal electronic devices on District premises or for accessing District resources is not permitted, however may be temporarily placed on the District's guest network. The Humboldt County School District is not responsible for the maintenance and security of personal electronic devices and assumes no responsibility for their loss or theft. The District reserves the right to enforce security measures on personal devices when used to access District tools and to remove devices found to be in violation of this AUP. Enforcement may include blocking access or requiring removal of unauthorized applications.

Energy Management

The Humboldt County School District strives to reduce our environmental footprint by pursuing energy conservation efforts and practices. The District reserves the right to adjust power-saving settings on electronics to reduce overall energy consumption. Devices may automatically enter hibernation mode after 15 minutes of inactivity as part of these conservation efforts.

Technology Purchasing & Donations

All technology hardware and software must be purchased or donated through the District's Technology Services Department unless prior approval has been received from the Technology Services Department and the Business Office. All technology purchases and donations must abide by District procurement policies and are subject to approval by the Technology Services Department. Technology pricing can include additional expenses required to ensure proper maintenance and security, including but not limited to warranties, hardware/software upgrades, virus protection, and security/inventory software.

Schools or departments applying for technology grants, funding, or donations must budget for any additional expenses associated with the requested technology and can be held responsible for any additional expenses incurred.

AUP Policy Review

Reviewed and Approved: This policy will be reviewed annually, no later than July 1 of each year, by the Humboldt County School District Administration, the Technology Director, the Superintendent's Office, and the Board of Trustees.

Distribution: Superintendent's Memo, Human Resources Department, Technology Department, posted on the District's official website, and the Student Handbook. Individuals may request a copy of this policy by contacting the District's Technology Services Department at (list contact information).

Revision: Requests for AUP amendments can be forwarded to the Humboldt County School District Technology Director for consideration. **Revision will be approved by the Superintendent's Office and the Board of Trustees.**

Approved: 11/26/2002
Revised: 09/2010; 9/13/2011; 7/22/2025