ACCEPTABLE USE POLICY FOR DISTRICT TECHNOLOGY RESOURCES

Scope of Policy

Hillsboro-Deering School District (HDSD) provides access to technology devices, Internet, and data systems to employees and students for educational and business purposes. This **Acceptable Use Policy (AUP)** governs all electronic activity of employees using and accessing the district's technology, Internet, and data systems regardless of the user's physical location.

Guiding Principles

- Online tools, including social media, should be used in our classrooms, schools, and central offices to increase community engagement, staff, and student learning, and core operational efficiency.
- HDSD has a legal and moral obligation to protect the personal data of our students, families, and staff.
- HDSD should provide a baseline set of policies and structures to allow schools to implement technology in ways that meet the needs of their students.
- All students, families, and staff must know their rights and responsibilities outlined in the Acceptable Use Policy and government regulations.
- Nothing in this policy shall be read 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.

Consequences of Breach of Policy

Use of all HDSD technology resources is a privilege, not a right. By using HDSD Internet Systems and devices, the user agrees to follow all HDSD regulations, policies, and guidelines. Students and staff are encouraged to report misuse or breach of protocols to appropriate personnel, including building administrators, direct supervisors, and to the **Office of Information Technology (OIT)**. Abuse of these privileges may result in one or more of the following consequences:

- Suspension or cancellation of use or access privileges
- Payments for damages or repairs
- Staff discipline under appropriate School District policies, up to and including termination of employment, subject to any collective bargaining obligations.
- Student disciplinary action, depending on the severity of the breach, could include a stern warning up to expulsion.
- Liability under applicable civil or criminal laws

Definitions

Freedom of Information Act (FOIA) - The FOIA is a law that allows for the release of government documents at the request of an individual. A FOIA request can be made to the Hillsboro-Deering School District for electronic documents/communications stored or

transmitted through district systems unless that information could be detrimental to governmental or personal interests. For more information, visit http://www.foia.gov/

Family Educational Rights and Privacy Act (FERPA) - The FERPA law protects the privacy, accuracy, and release of information for students and families of the Hillsboro-Deering School District. personal data stored or transmitted by agents of the Hillsboro-Deering School District must abide by FERPA laws, and HDSD is required to protect the integrity and security of student and family information. For more information, visit http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

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 Hillsboro-Deering 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.

Communication & Social Media

Employees and students are provided with district email accounts and online tools to improve the efficiency and effectiveness of communication, both within the organization and with the broader community. Communication should be consistent with the professional practices used for all correspondence. When using online tools, members of the HDSD community will use appropriate behavior:

A. When acting as a representative or employee of the Hillsboro-Deering School District.
B. When the communication impacts or is likely to impact the classroom or working environment in the Hillsboro-Deering 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 school business is strongly discouraged and may open an individual's personal account to be subject to FOIA inquiries. HDSD 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 school district policies or government regulations.

Guidelines for Online Communication

- Communication with students should not 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 that 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 (blogs, Twitter, etc.) are expected to refrain from discussing confidential information and/or discussing specific students. Information that can be traced back to a particular 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.
- Employees are required to notify their appropriate administrator 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 students/former students or parents as 'friends' or contacts on social media unless the site is expressly set up to support classroom instruction or school business.
- Employees may communicate with HDSD graduates (+18 years old) on social media but should be advised to maintain professionalism and caution when communicating online.
- Employees are encouraged not to add parents/guardians of students as 'friends' or contacts on social media to maintain professionalism and to avoid any appearance of a 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: HDSD 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 OIT Help Desk.

Solicitation

The HDSD prohibits web announcements and online communication promoting a business. The Superintendent's Office may make exceptions if benefits are judged sufficient to merit exception.

Use of Copyrighted Materials

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

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

Network Usage

Network access and bandwidth are provided to schools for academic and operational services. HDSD reserves the right to prioritize network bandwidth and limit certain network activities that are negatively impacting academic and operational functions. Users are prohibited from using the HDSD 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 in the Children's Internet Protection Act (CIPA), HDSD is required to protect students from online threats, block access to inappropriate content, and monitor the Internet use by minors on school networks. OIT is responsible for managing the district's Internet filter and will work with the HDSD 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, HDSD 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 HDSD network or in HDSD systems. HDSD reserves the right to access, review, copy, store, or delete any files (unless other restrictions apply) stored on HDSD computers and all employee and students communication using the HDSD network. Electronic messages and data stored on HDSD computers or transmitted using HDSD 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. HDSD may choose to deploy location tracking software on devices for the sole purpose of locating devices identified as lost or stolen.

Personal Use

HDSD recognizes that users may use HDSD email, devices, and network bandwidth for limited personal use; however, personal use should not interfere with or impede district business or cause an additional financial burden on the district. Excessive use or abuse of these privileges can be deemed in violation of the Acceptable Use Policy.

Network Security

The HDSD Wide Area Network (WAN) infrastructure, as well as the building-based Local Area Networks (LANs), are implemented with performance planning and appropriate security measures in mind. Modifications to an individual building network infrastructure 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 OIT 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 Information Security Officer.

Data & Systems

Access to view, edit, or share personal data on students and employees maintained by HDSD 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. 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 or non-HDSD individuals requesting protected data must receive approval from the Office of the Legal Advisor and have a non-disclosure agreement with the HDSD. Individuals requesting ongoing access to data through HDSD systems are required to have a designated HDSD administrator who will act as a "sponsor" to ensure the safety 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 HDSD systems to transmit data. Staff are also expected to ensure records are sent only to individuals with a right to said records and must take reasonable measures to ensure that only the intended recipients can access the data.

Passwords

Users are required to adhere to password requirements set forth by the Hillsboro-Deering 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 (USB devices, hard drives, CDs, flash drives, etc.) with sensitive data must be securely protected with a password and encrypted to ensure the safety of the data contained. OIT must approve the use of cloud-storage services for storage or transmission of files containing sensitive information. Users are encouraged to use HDSD approved data/information systems for the storage and transmission of sensitive data whenever possible and avoid storage on local hardware that cannot be secured.

Electronic Devices

HDSD defines electronic devices as, but not limited to, the following:

- Laptop and desktop computers, including like-devices
- Tablets
- Wireless email and text-messaging devices, i.e., iPod
- Smartphones
- Donated devices

Device Support

HDSD provides necessary installation, synchronization, and software support for HDSD-issued electronic devices. Devices must be connected to the HDSD network regularly to receive up-to-

date software and antivirus updates and for inventory purposes. Password protection is required on all HDSD-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.

Loss/Theft

Users must take reasonable measures to prevent a 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 their direct supervisor, local authorities, and the OIT). The HDSD will take all reasonable measures to recover the lost property and to ensure the security of any information contained on the device.

Return of Electronic Devices

All technology purchased or donated to the HDSD is considered district property, and all equipment assigned to employees or students must be returned before leaving their position or school. All equipment containing sensitive information and data must be returned directly to OIT before it can be redeployed.

Personal Electronic Devices

The use of personal electronic devices is permitted at the discretion of the appropriate administrator and Information Security Officer. The HDSD is not responsible for the maintenance and security of personal electronic devices and assumes no responsibility for loss or theft. The district reserves the right to enforce security measures on personal devices when used to access district tools and remove devices found to violate the AUP.

Energy Management

HDSD 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 energy consumption.

Technology Purchasing & Donations

Technology hardware and software must be purchased or donated through OIT, unless OIT and the Business Office have granted prior approval. All technology purchases and donations must abide by HDSD procurement policies and are subject to approval by OIT. 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 costs incurred.

Legal References:

15 U.S.C. §§ 6501-6506 Children's Online Privacy Protection Act (COPPA)
20 U.S.C. § 1232g Family Educational Rights and Privacy Act (FERPA)
20 U.S.C. § 1232h Protection of Pupil Rights Amendment (PPRA)
20 U.S.C. § 1400-1417 Individuals with Disabilities Education Act (IDEA)
20 U.S.C. § 7926 Elementary and Secondary Education Act (ESSA)

20 U.S.C. §6777, Enhancing Education Through Technology – Internet Safety
47 U.S.C. §254, Requirements For Certain Schools – Internet Safety
RSA 189:65 Definitions
RSA 186:66 Student Information Protection and Privacy
RSA 189:67 Limits on Disclosure of Information
RSA 189:68 Student Privacy
RSA 189:68-a Student Online Personal Information
RSA 194:3-d, School District Computer Networks
RSA 359-C:19-21 Right to Privacy/Notice of Security Breach

Policy Adoption & Revision History:
Policy Committee Review: 6/13/19, 9/17/19
Replaces GBEF Staff Acceptable Use Policy for District Networks, Electronic Devices and Internet 6/20/11; JICL Student Acceptable Use Policy for District Networks, Electronic Devices and Internet 3/21/11; and KD School District Social Media Sites 8/15/16
First Reading: 10/07/19
Second Reading: 10/21/19
Final Approval: 11/14/19
Policy Committee Review: 2/22/24 (no change)