High Desert Education Service District

Code: IIBGA-AR
Adopted: 5/29/01
Revised/Reviewed: 9/19/06, 1/18/11
8/22/16, 9/26/17

Electronic Communications System

High Desert Education Service District (HDESD) recognizes the important role of technology in enhancing the work we do for students and our communities. HDESD staff are encouraged to use information and technology resources to improve excellence, equity, and efficiency in their work.

PURPOSE

The purpose of the High Desert Education Service District Responsible Use Policy (RUP) is to provide guidelines, rules, and the code of conduct for the use of information and technology resources, the HDESD network, and other connected networks including the internet. We provide these guidelines and rules to ensure the safety of staff, students, parents and technology systems.

There are two important notes before the policy continues:

1. User Responsibilities
   HDESD staff are required to read and understand this RUP before accessing HDESD information and technology resources. Staff will acknowledge, by digital or written form, they have read and will comply with the RUP. HDESD staff with questions regarding the application or meaning of this RUP are encouraged to communicate with the Chief Information Officer to obtain clarification.

2. Expectation of Privacy
   HDESD staff are required to read and understand this RUP before accessing HDESD information and technology resources. Staff will acknowledge, by digital or written form, they have read and will comply with the RUP. HDESD staff with questions regarding the application or meaning of this RUP are encouraged to communicate with the Chief Information Officer to obtain clarification.

   HDESD staff are reminded there is no expectation of privacy when using HDESD information and technology resources. HDESD reserves the right to disclose any electronic messages to law enforcement officials or third parties as appropriate. All documents and communication are subject to the public records disclosure laws of the State of Oregon, e.g. ORS 192.410.

RESPONSIBLE USE

In addition to the general use of information and technology resources, staff are encouraged to use digital tools to communicate with colleagues, students, and parents/guardians, subject to appropriate consideration for student privacy. Digital communications are often public in nature; therefore, general rules and standards for professional behavior and communications will apply. HDESD staff are reminded the use of information and technology resources is subject to the same management oversight as other employee activities.

Responsible use of HDESD information and technology resources by staff includes, but is not limited to, the following:

- using HDESD-owned hardware, software, network, and internet connectivity to work efficiently;
- accessing the internet to retrieve information for use in operations and instruction;
- communicating using email and messaging applications;
- maintaining and safeguarding passwords; changing passwords regularly;

- acting as positive representatives of HDESD while on the internet;
- conducting online activities in an ethical and legal fashion;
- abiding by generally accepted rules of network etiquette; and,
- notifying the technology department if you learn others are utilizing HDESD information and technology resources for unlawful or suspicious activities.

ACCESS

All staff members are authorized to use HDESD information and technology resources within the limitations established by Board policy and this RUP. The district will monitor electronic communication use, including internet and email use.

E-mail Access

Each HDESD employee will be provided an HDESD e-mail address. Email is the primary source for agency-wide communications and will be relied upon to communicate announcements, changes in procedures, and other important information. Each employee is expected to access email on a regular basis.

Hardware and Software Access

Each HDESD employee will be provided hardware and software to meet the needs of the work assigned, in consultation with and approval of the employee supervisor or program manager. We will match needs with desktop computers, laptop computers, mobile devices, and/or a range of productivity software.

Internet Access

The use of the internet while at work should support the educational, instructional, and operational goals of our organization. This includes accessing web sites, search engines, productivity tools, communication tools, social media, and email. HDESD staff will use good network etiquette. Examples of good etiquette include the following:

- Be polite.
- Use appropriate language. Do not swear, use vulgarities, or any other inappropriate or suggestive language. Do not be abusive in your messages to others.
- Do not break the law. Illegal activities are strictly forbidden. (Remember that staff have no expectation of privacy while using their HDESD-provided email accounts and the internet. Technology staff who operate the system have access to all mail. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.)
- Do not reveal your personal address or phone number or that of other employees or students, except in your normal course of duties.
- Do not disrupt the use of the network by other users. (This can happen when downloading large movie files or with some streaming media services.)
- Do not download and use copyrighted material without the written permission of the copyright holder.

Wireless Internet Access

It is permissible to access HDESD wireless internet where available using any personal computing device. However, access of the wireless internet by staff means that the user agrees to all the rules and guidelines set forth in this document.

Personal Internet Access

Occasional and incidental personal use of HDESD information and technology resources and internet access is allowed subject to the following limitations.

Personal use of the internet is prohibited if:

- It materially interferes with the use of information and technology resources by the district; or
- Such use burdens the district with additional costs; or
- Such use interferes with the staff member's employment duties or other obligations to the district; or
- Such personal use includes any activity that is prohibited under any district procedural directive.

MOBILITY

HDESD recognizes mobile devices improve communication and efficiency. We will continue to build information systems that are compatible with mobile devices, smaller screens, and a variety of connection speeds.

Mobile Devices

Employees issued an HDESD mobile device shall have no expectations of privacy with respect to the content on the device. This includes, but is not limited to, internet usage, phone calls, text messages, photos, email, notes, and applications. Prohibited activities outlined in this RUP shall apply to activity on district mobile devices.

District mobile devices and related content are subject to provisions of the Oregon public records laws, including any personal information that may be housed on the district mobile device. Pursuant to Oregon statutes, public records may not be intentionally destroyed once the information has been formally requested.

Employee personal mobile devices may also be subject to Oregon public records laws, if the employee has engaged in HDESD business on their personal device.

Mobile Device Administrator Permissions

Employees who access HDESD information services, e.g. email, using a mobile app on their personal mobile device will be asked to grant security administrator access to their device in the event of device theft, loss, or HDESD data that is in any other way compromised. This access does not allow a system administrator to view content on your device. It allows the system administrator to suspend your device's connections to HDESD services or, in the case of theft or loss, to wipe your device.

SECURITY

Password-protected accounts are the first level of security for access to HDESD information and technology resources. System logins and accounts are to be used only by the authorized owner of the account for authorized district purposes. Staff are responsible for all activity on their account, must not share their account password, must not use the account of other users, and must exercise responsible password management, including password changes at regular intervals.

Privacy

Staff should not reveal personal information, including a home address and phone number on websites, blogs, podcasts, videos, social networking sites, wikis, email or as content on any other electronic medium.

Staff should not reveal personal information about another individual on any electronic medium without first obtaining permission.

Student Information Privacy

HDESD staff who have access to personally identifiable student records shall adhere to all standards included in the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), and other applicable laws and regulations, as they relate to the release of student information.

Staff will follow student data privacy regulations and HDESD information security processes when sharing confidential or sensitive information, student data, or any other information covered by existing state or federal privacy or confidentiality laws, regulations, rules, policies, procedures or contract terms.

Social Media

HDESD staff should exercise caution and common sense when using HDESD or personal social media.

Employees are prohibited from inappropriate online socializing with students or from engaging in any conduct on social networking web sites that violates the law, district policies, or other generally recognized professional standards. Employees whose conduct violates this policy may face discipline or termination, consistent with board policies, responsible use agreement, and collective bargaining agreements, as applicable.

HDESD staff are encouraged to use appropriate privacy settings to control access to their personal social media sites, although there are limitations to privacy settings. Private communication published on the internet can easily become public; social media sites can change current default privacy settings and other functions. As a result, employees have an individualized responsibility to understand the rules of the social media site being used.

Filtering and Monitoring

Filtering software is used to block and/or filter access to visual depictions that are obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA). Filtering software is not 100% effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a complete solution. HDESD staff must take responsibility for their use of the network and internet and avoid objectionable sites.

PROHIBITED ACTIVITIES

HDESD encourages staff to use information and technology resources responsibly. This policy was updated in August 2016. Technology plays a significant role in the communication we share and the work we do. The restrictive IT policies from decades before have been replaced with encouragement and guidelines for the integration of these tools into our workflow.

- Staff shall not use the network to transmit profane, obscene, vulgar, sexually explicit, threatening, defamatory, abusive, discriminatory, harassing, criminal or otherwise objectionable messages or materials. (Employees are also prohibited from visiting internet sites that post such materials and downloading or displaying such materials.)
- Staff shall not upload or otherwise transfer out of the district's direct control any software licensed to the district or data owned or licensed by the district without explicit written authorization.
- Staff shall not use HDESD information and technology resources for personal gain, commercial solicitation or compensation of any kind.
- Staff shall not use HDESD information and technology resources to support or oppose ballot measures, candidates and any other political activity.
- Staff shall not use HDESD information and technology resources to intentionally disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of the district's information technology resources.
- Email shall not be utilized to share confidential information about students or staff without authorization.
- No staff member may disclose, use, or disseminate any personal information regarding students or staff without authorization.
- Generally, the same standards of acceptable staff conduct which apply to any aspect of job performance shall apply to use of HDESD information technology resources.