Information Technology
Policies and Procedures

Table of Contents

Summary and Annual Notification

The purpose of this document is to inform users of HUSD computer and network resources about policies and procedures in place affecting the use of such technology. This page (only) is to be included in the annual notification to all employees and students, with a reference to the full document posted on the District's web site (http://www.hemetusd.org/ourpages/IT/IT Policies and Procedures.pdf) By signing the annual notification receipt form, users acknowledge the following:

Acceptable Use:
The purpose of using the Internet in our school system is to support research and education by providing access to unique resources and the opportunity for collaborative work. The use of on-line services must be in support of education and research and consistent with the educational objectives of the Hemet Unified School District. Transmission of any material in violation of school policy or any U.S. or state regulation is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, and material protected by trade secrets.

Expectation of Privacy:
All communications and information accessible via the network should be assumed to be property of Hemet Unified School District and subject to district guidelines and policies.

Data Confidentiality and Passwords:
All users are responsible to maintain the confidentiality of records and information, both for students and for staff. Do not share your password with anyone. Do not use another individual's account. Attempts to log onto the network as anyone but yourself may result in cancellation of user privileges and disciplinary action. Students may not access a device logged in under a staff user account in such a way that a student may access data or services intended for staff use only.

Personal Equipment on the District Network:
The use of any unauthorized personal devices or network equipment on the HUSD network is prohibited. Personal devices may be connected to the HUSD provided guest wireless network if one is available.

Equipment Loans to Employees:
The staff member will be financially responsible for damage or loss to loaned equipment while the equipment is away from the site. Also, the loaned equipment may only be used for school-related tasks, and it may not be used for personal reasons.

Document and File Storage:
Documents and files of a personal nature may not be stored on the network resources provided by the district. In addition, users are responsible to abide by all laws and regulations regarding copyright and intellectual property, and they are solely responsible for any copyright violations.

Installing Software & Hardware on District Computers:
To help maintain the integrity of our network and computers, ONLY "district approved" hardware or software is allowed on the network or district computers. DO NOT attempt to install any hardware or software on your own, always contact the Help Desk.

Web and SPAM Filter:
HUSD has a web filter in place to ensure students/employees are not visiting inappropriate web sites. Google (Gmail) has a SPAM filter that filters e-mails based on sender address and content. The filter will block any e-mails from known SPAM sources or with content that includes words found in sales messaging, etc.

Introduction

The District offers employees, students, and district collaborators (on MOU/contract) access to the District's computer network and the internet. The policies and procedures described below apply to employees and students granted network and Internet access by the District. For the District to continue to make network and Internet access available, students and staff must behave appropriately and lawfully. By using the network and application account(s) issued to you, you acknowledge that you will abide by all applicable District policies and procedures, laws, IT Policies and Procedures, and / or site or department rules.

If you or anyone you allow access through your account (itself a violation of District Policies) violates any applicable District policies and procedures, laws, IT Policies and Procedures, and / or site or department rules, your access may be denied or withdrawn. In addition, you may be subject to disciplinary action, criminal prosecution, or both.

All communications and information accessible via the network should be assumed to be property of Hemet Unified School District and subject to district guidelines and policies.

I.   Acceptable Use

The purpose of using the Internet in our school system is to support research and education by providing access to unique resources and the opportunity for collaborative work. The use of on-line services must be in support of education and research, and consistent with the educational objectives of the Hemet Unified School District. Transmission of any material in violation of school policy or any U.S. or state regulation is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, and material protected by trade secrets."

II.   Expectation of Privacy

All activities on district electronic resources are subject to monitoring. Employees, students and district collaborators acknowledge this by signing the appropriate Electronic Information Resource User Contract. In addition, the IT department has implemented the following login banner for all standard computer systems, which must be acknowledged by the user prior to logging on.

> "Welcome to the Hemet Unified School District Network.
>
> This banner serves as a reminder for all computer users to adhere to the Acceptable Use Policy. Please use the network appropriately at all times for school and business purposes only.
>
> As an employee of Hemet Unified School District, you are required to be aware of and abide by the Acceptable Use Policy.
>
> The Acceptable Use Policy per BP/AR 6163.4 was signed and/or received by all Hemet Unified School District employees and students.
>
> Thank You"

In addition, electronic documents and communications are District records. As such, they may be subject to Public Information Act requests and may be subpoenaed in case of litigation.

III. Data Confidentiality and Passwords

All users are responsible to maintain the confidentiality of records and information, both for students and for staff. User passwords are critical in maintaining the integrity and confidentiality of systems, applications, and information. Per the Acceptable Use Policy users shall:

- Logon to systems and applications only when using those systems and applications.
- NOT leave their computer unattended or unlocked.
- Logout and shut down their computer at the end of their work /school day.
- Access systems and information only under their user account.
- NOT allow students to use systems, applications, and information, unless students are using their own login credentials or other appropriate login account.
- NOT share passwords with other users
- NOT write down user names and / or passwords (IT staff can help with forgotten passwords).
- NOT allow other users access to systems, applications, and information, unless those users are authorized to do so and are using their own login credentials.
- NOT reveal personal addresses or phone numbers or other personal information of students or colleagues.
- NOT use the network in such a way that you would disrupt the use of the network by other users.

Users are required to change passwords at regular intervals. We strongly discourage users from writing down passwords for future reference.

IV. Personal Equipment on the District Network

HUSD provides secured network access as well as guest network access. The guest network access provides filtered Internet access only.

HUSD provides guest network access for mobile personal devices such as laptops and tablets. This guest access is only available via a designated guest wireless network. There is no hard wired guest access and therefore personal devices should not be connected to any data wall jack. Any personal devices accessing the HUSD guest network or cellular networks MUST conform to the HUSD Acceptable Use Policy.

The use of any personal computers or network equipment on the HUSD secured network is prohibited. This includes, but is not limited to:

- Desktop computers
- Laptops
- Tablets
- Wireless access points
- Routers
- Switches/Hubs
- Multimedia equipment
- Security equipment/cameras
- Any network capable devices

The introduction of unmanaged or improperly configured devices can pose a serious risk to the security of the District network and the integrity of the data we maintain. Wireless access points and routers are also serious threats to network integrity. They can potentially allow unauthorized wireless connections to our network, even from outside the campus, and bypass our security measures. Due to this extreme risk, any

unauthorized access points, routers, switches, or other devices functioning in such a manner as to affect network connectivity or security are subject to immediate confiscation.

V. Equipment Loans to Employees

As the use of mobile devices proliferates throughout the District, it is important for the sites to maintain accurate account of equipment that users may be taking home with them. School sites are responsible to check equipment out and in, and to obtain the appropriate signatures from staff members.

Please keep in mind the following:

- The District / sites do not purchase accidental damage or loss protection for mobile devices. The staff member will be financially responsible for equipment damage or loss while the equipment is away from the site.
- Staff may not load any programs or software on the devices other than programs for which the District or the site owns a license for and has been previously approved for use though the software approval process.
- The devices must be brought in to the office / classroom and connected to the District network on a regular daily or weekly basis. This is necessary to ensure that systems are kept up to date, including anti-virus and anti-spyware definitions, software updates, and user and computer policies.

VI. User accounts

Types of Accounts Managed by IT

The IT Department creates, manages, and updates the following types of accounts:

- Network accounts. These user names and passwords are used to access the local computer and resources on the District networks, including home directories and shared resources.
- Aeries accounts. These accounts are used to access the District's student information system.
- Email accounts. These accounts are used for e-mail and calendaring.

The following are some of the accounts that are NOT managed by IT. All inquiries regarding these accounts should be directed to the appropriate department.

System or Application	Description	Accounts managed by
All The Right Type Online	Typing Tutor online	Professional Development
Apex	Online Credit Recovery	Site coordinator
Benefit Bridge	Benefit system	Benefits Department
Bluebear SchoolBooks & Tracks	Accounting system	Fiscal Services
Compass Learning	Student performance and testing	Professional Development
Destiny	Library / textbook system	District Librarian
Data Director	Student performance and testing	Special Programs
Edlio	Site Web sites	Site coordinator
eFT Web Field Trips	Field Trip scheduler	Transportation
SBAC	Student performance and testing	Special Programs
Galaxy	Accounting system	Fiscal Services
Go Sign Me Up	Event registration system	Professional Development
PowerSchool (Haiku)	LMS	Professional Development
Keenan Safe School	Safety system	Safety Department
MAP	Student performance and testing	Special Programs
OneSource	Purchasing system	Purchasing
STMath	Student performance and testing	STMath
School Dude	Work order system for M&O	Maintenance & Operations
School Stream	Approval system	Fiscal Services
Absence Management (Aesop)	Employee attendance system	Human Resource
Talent Ed	EVAL system	Human Resource
Typing Pal	Typing Tutor online	Professional Development

Who Can Get an Account?

For accounts managed by IT, the following chart shows who may be issued the various types of accounts. Keep in mind that staff accounts should be requested only when the type of access is necessary for the staff member's performance of their duties, and the request must be approved by the Human Resources Department or employee's supervisor or other administrator when appropriate. All new account requests must be sent via e-mail to the IT Help Desk (helpdesk@hemetusd.org) with the legal full name, site, title, and employee ID number.

Accounts will not be issued for non-employees of the District, unless specified below.

	Network	Aeries	Email
Employees			
Administrators	Yes	Yes	Yes
Staff	Yes	Yes	Yes
Teachers	Yes	Yes	Yes
Subs Long Term (30 days or more)	Yes	Yes	Yes
Subs (less than 30 days)	No	No	No
Students			
Grades 9-12	Yes	Yes	Yes
Grades 6-8	Yes	Yes	Yes
Grades 3-5	Yes (generic)	Yes	No
Grades K-2	Yes (generic)	No	No
Other			
SRO/DA/Probation Officers	Yes	Yes	Yes
Contracted SpEd providers working at the school sites	Yes	Yes	Yes

Accounts for other contracted providers, such as auditors, consultants, contractors, etc., may be created at the discretion of management as defined by MOU and/or contract.

Access Hours

It is necessary to limit the access hours of certain systems and applications to allow for the successful backup of data and other nightly procedures. This limit also protects systems, applications, and information from unauthorized access after-hours. Access hour limitations are as follows:

Employees	Monday—Sunday 5:00 AM—6:00 PM
Students	Monday—Saturday 5:00 AM—6:00 PM
Adult Ed Employees & Students	Monday—Saturday 5:00 AM—10:00 PM
E-mail	24/7

Account Expiration

Due to the confidential nature of personal data contained within our network system and to protect HUSD from potential cyber-attacks and security breaches, the IT Department has developed an expiration policy for user accounts. The expiration of an account does not automatically delete the account. Expiration of an account prevents it from being used until appropriate action is taken by IT to either delete the account or remove the expiration. The expiration policy activates after a user account has been inactive for over 60 days.

It is highly recommended that once a staff receive an HUSD network and e-mail account, that staff needs to reset their password as soon as possible and to secure their new password. It is also highly recommended that staff access their e-mail account prior to the 60 days expiration policy. A good practice is to check your e-mail account at least once a month.

All network and e-mail accounts will be expired as follows:

Permanent employees	Upon termination of employment or if an account is inactive for over 60 days
Students	The end of the current school year
Temporary employees or long-term substitutes	The expected end date of their assignment, or the end of the current school year, whichever comes first
Other	The expected end date of their assignment, or the end of the current school year, whichever comes first

Account Deletion and Document Archiving Rules

All expired employee accounts will be deleted no sooner than thirty days from the expiration date (for accounts inactivated after July 1, the deletion will occur no sooner than thirty days after the beginning of the new school year). This allows time to reactivate accounts that were expired erroneously or that should be reinstated for any other reason. Once an account is deleted, the user's home directory is archived and retained for up to six months. After that, all documents in the home directory are purged.

Student accounts for non-returning students are deleted over the summer, and their home directories are purged after 30 days.

Inactive Accounts

Staff network and e-mail accounts are considered inactive when the user has not logged on using that account for at least sixty days (over the summer, accounts are deemed inactive when not used within the first sixty days of the new school year). The IT Department runs account activity reports on a regular basis to identify inactive accounts.

Inactive staff accounts are subject to being expired. Once an inactive account is expired, the account deletion and archiving rules will apply as described in the previous section.

VII. Document and File Storage

Home Directories and File Backups

The user's home directory is a location on a network resource where the user can save documents. Saving documents to the home directory serves two purposes: (1) allow the user access to his/her documents from another computer, and (2) protect the user's documents in case of failure or malfunction of his/her computer.

In addition to the user's home directory, some users may have access to shared storage to collaborate with others on the network.

Employees must be aware that any documents NOT stored in either the home directory or a shared folder will NOT be backed up. This includes documents stored on the local computer drives (including the desktop). In the event of equipment failure or malfunction, files stored on the local computer may be permanently damaged or lost. IT will only provide assistance in recovering files and documents stored in the employee's home directory or in other shared folders provided by IT.

Network Storage

Because network storage space is finite, and adding network storage can be expensive, the following types of files or documents may NOT be stored in the user's home directory or any of the shared folders provided by IT and may not be included in nightly backups:

- Programs (e.g., executables [.EXE, .COM])
- Photographs, music and videos (unless necessary to perform the employee's duties or for instructional purpose, or for student use in class projects).
- Personal files of any kind

VIII. Installing Software on District Computers

Before any program or software can be installed on a district, department, or school computer, the appropriate license must be obtained by the district, department, or school. Any software must be approved by the IT Department prior to its acquisition and installation. In addition, instructional software must be approved by either Educational Support Services or Student Support Services. In either case, the IT Department needs an opportunity to test the proposed program or software to make sure it is compatible with our environment. All software must be approved via a documented software approval process.

Users may not install programs and software on district, department, or school computers unless expressly authorized to do so, regardless of technical capability to do so. Users are responsible for observing BP and AR 6162.6 Use of Copyrighted Materials and any applicable laws and regulations regarding intellectual property.

IX. Web Filter

Users acknowledge that the District cannot guarantee the accuracy of the information or the appropriateness of any material they may encounter using the Internet.

The District uses a filter appliance to control access to inappropriate web sites and web content. The purpose of this filter is to protect students and staff from harmful content, such as pornography or nudity. The filter is also used to enforce District policies and procedures regarding acceptable use.

While some sites may not be considered "harmful", they may still be blocked in order to preserve bandwidth or to focus the use of technology for instructionally appropriate purposes, or for use related to the business of the District.

Sites are sometimes incorrectly categorized as inappropriate. If you discover that a site you need for school or business related purposes has been blocked in error, contact the IT Help Desk.

Web browsing is logged by user and computer. This record includes, among other information, web sites visited, blocked requests, duration of visit, and bandwidth used. The appliance automatically authenticates users on supported machines in order to log browsing by user, rather than by machine. This authentication is transparent and happens through your network login.

It is a violation of District policy to attempt to use sites known as proxies, anonymizers, translators, or any other site or tool for the purpose of bypassing the District's established filter.

Under certain circumstances and under the direction of the Human Resources department, school site or district office administrators may request specific reports pertaining to employee or student internet activity and usage for evaluative or disciplinary purposes.

Periodically, the IT Department will review the Internet Access log. Any inappropriate access may be reported to the site administrator and/or Human Resource Department.

X. SPAM Filter

HUSD does not manage the spam filter. Google (Gmail) controls SPAM Filtering, however Gmail users can Report SPAM email directly to Gmail SPAM Filters within Gmail.

XI. Donations

The Hemet Unified School District welcomes and accepts suitable donations of computer equipment and peripherals.

A basic principle of controlling the Total Cost of Ownership (TCO) of technology in our schools is that the greater the standardization within our computer network, the lower the costs of operating it, in terms of the needs for technical support, parts inventory and staff development. (Please visit the CoSN web site for more information regarding computers and networks in schools). This, along with the increasing requirements to properly dispose of computer equipment, and the associated cost, has resulted in the development of the following guidelines for computer donations:

1. The preferred method for donating computers to our schools is a monetary donation earmarked for the purchase of computer equipment that meets our established hardware and software standards. Schools may use the monetary donation to purchase new or refurbished equipment that meet our District standards.

2. If a monetary donation is not possible, the donated equipment needs to meet the following minimum requirements:

   Dell OptiPlex 990 Desktop

   - Microsoft Windows 7 Professional
   - Intel Core i5 Processor
   - 120GB or larger SSD
   - 8GB of RAM
   - 10/100/1000 Network card
   - Dual monitor support
   - DVD +/- RW (optional)
   - Dell 19" or larger LCD monitor
   - Dell USB keyboard & Mouse

Dell Chromebook 11 3120, 3180, 3189

- 16GB Internal Storage
- 4GB RAM
- Chrome OS version 57 or newer

3. For suitable donations, the school site must submit a purchase request for a license of the then-current version of Microsoft Windows OS and Microsoft Office Suite. If the computer does not meet the memory (RAM) requirement, the site must also submit a purchase request for the additional memory to bring the system up to the above level. Due to strict copyright laws regarding computer software and other intellectual materials, the donated computer hard drives must be fully erased.

4. Any computer donation that does not meet the above standard may be considered on a case-by-case basis under the following guidelines:

   - Equipment may not be connected to the school / district network.
   - Setup, support and maintenance of this equipment are the responsibility of the school.
   - The school site has outlined a specific use for the equipment as a standalone system (not connected to the network.)
   - The school site will submit a purchase request for all appropriate software licenses.

XII. Obtaining Support for Computer Problems

There are currently two methods to obtain support for general computer problems in HUSD:

1. Contact IT Help Desk via email (helpdesk@hemetusd.org) to submit your support request. Please provide as much specific information as you can about the issue you are having.

2. Please contact the IT Help Desk by calling 765-5100 x.5580. To obtain the most efficient service please keep the following in mind:

   - Help Desk operating hours are Monday-Friday 7am-5:00pm.
   - We ask that the actual user who is experiencing the problem make the call, and from the problem computer. This allows us to troubleshoot (and often correct) the problem over the phone or by remote controlling the PC in question.
   - Please call ONLY the provided Help Desk number for assistance as those technicians are best equipped to answer most of the problems you may experience. Please do not "phone shop" to try to get assistance from another IT staff member.
   - If you are asked to leave a message, it means the technicians are helping other users – please leave a detailed message with your name, site, problem, call back number and the best time to reach you. Please do not leave multiple messages.
   - If your site is experiencing an emergency/high priority issue, please notify your school office and they will contact IT directly.

XIII. Technology Supported Hardware

 IT Help Desk supports most hardware and troubleshoot most issues. The following list provides users a guide of Fully Supported, Partially Supported and Not Supported by IT Help Desk. This applies to District-owned devices only as we do not support personal devices.

Desktops	Fully Supported	including monitor, keyboard, mouse and District approved software
Laptops	Fully Supported	complete hardware and District approved software
Servers	Fully Supported	District servers
Network	Fully Supported	Network infrastructure equipment, data jacks and cabling
Access Points	Fully Supported	Wireless infrastructure equipment
Printers	Partially Supported	Setup, drivers, connection and troubleshoot. DO NOT REPAIR
Scanners	Partially Supported	Setup, drivers, connection and troubleshoot. DO NOT REPAIR
Projectors	Partially Supported	Setup, drivers, connection and troubleshoot. DO NOT REPAIR
Doc Cameras	Partially Supported	Setup, drivers, connection and troubleshoot. DO NOT REPAIR
Tablets	Partially Supported	Provide wireless access only; and network management/tracking.
Chromebooks	Fully Supported	Wireless network connection, troubleshooting, hardware repair and/or replacement (Dell Chromebook 11 3120, 3180, 3189 models only)
Phones	Not Supported	Provide wireless access only

XIV. Aeries Student Information System

User Accounts

Logging In (Staff, Teacher, and Student Accounts)

Hemet Unified uses Google Single Sign-on to login to Aeries. This means that your google login for Gmail, Google Docs, etc. is also your login for Aeries. There is no need to keep track of a separate password. Staff and Teachers can login to the Aeries website at https://aeries.hemetusd.org. Students and parents can login to the Aeries Portal at https://portals.hemetusd.org.

Staff Accounts

Staff Accounts for Aeries are created by the IT Aeries Support Team once Human Resources has requested an account be created. This allows HR to provide both verification of valid employment and the staff members information, including legal first name, last name, and staff id.

Teacher Accounts

Teacher Accounts are created by the IT Aeries Support Team once Human Resources has added the staff member to the Staff Area of Aeries. Once this is completed, the Office Manager adds the teacher to the school location. This assigns a local teacher number the system uses for attendance and grading.

Student Accounts (3rd – 12th grade)

Student accounts are created automatically on a nightly basis for third grade and up. This means a student can login to the Aeries student portal the next day after becoming an active student in Hemet USD. Student accounts are created using the students first initial, last initial and student id. For Example, John Doe with id 123456 would have a login id of jd123456@stu.hemetusd.org

Parent Accounts

Parents will need to create their own personal accounts to the portal. This account can be used for online re-registration and viewing their students attendance and grades. In order to create a portal account, the parent will also need to contact the school to receive their student's verification code. This code prevents individuals from creating an account and monitoring children they are not directly related to.

Parent Portal

The Parent Portal allows parents to monitor their child's attendance and grades. Parents can login anytime day or night to see the current status of their child's academic situation. This allows parents to take a more active role in their child's education.

Parents have the option of configuring features on the portal to efficiently monitor their children's progress. These features are Weekly Progress Email and Alert Threshold Email. The Weekly Progress Email allows a parent to configure the portal to send an email weekly that outlines their child's current grades. It can be configured for any day of the week the parent desires. The Alert Threshold Email allows parents of Middle and High school students to create an upper and lower grade they wish to be notified about. For example, if the lower threshold is set to D, then the parent will receive an email when their child's grade drops to a D.

XV. Web Accessibility Notice

Hemet Unified School District provides equal access to education, employment, services, programs, and activities to persons with disabilities. The HUSD community works together to remove any barriers that prevent equal opportunities to community members who have physical or mental disabilities.

We are committed to providing services to comply with Section 504 and Section 508 of the Rehabilitation Act of 1973 and Title II of the Americans with Disabilities Act of 1990.

Section 508 requires that all website content be accessible to people with disabilities. This applies to web applications, web pages, and all attached files on the internet. Section 508 requires that individuals with disabilities have access to and use of information and data that is comparable to those who are not individuals with disabilities.

Help with Accessibility

Many popular browsers contain built-in accessibility tools:
Google Chrome Accessibility Information
Internet Explorer Accessibility Information
Firefox Accessibility Information

If you have trouble accessing any of our webpages or documents, please send an email to accessibility@hemetusd.org. Please help us respond to you in the most beneficial way by indicating the nature of your accessibility problem, the preferred format(s) in which you want to receive the material, and your contact information.

Additional contact information is listed below:

Phone: (951) 765-5100 Ext. 5590
Email: accessibility@hemetusd.org