

Network Access General Use Policy for Staff

Guidelines for Acceptable Use of West Hardin C.C.I.S.D. Technology Resources

2009-2010

The West Hardin County Consolidated Independent School District provides technology resources to its students and staff for educational and administrative purposes. The goal in providing these resources is to promote educational excellence in the District's schools by facilitating resource sharing, innovation and communication with the support and supervision of parents, teachers and support staff. The use of these technology resources is a privilege, not a right.

With access to computers and people all over the world comes the potential availability of material that may not be considered to be of educational value in the context of the school setting. West Hardin C.C.I.S.D. firmly believes that the value of information, interaction, and research capabilities available outweighs the possibility that users may obtain material that is not consistent with the educational goals of the district.

Proper behavior, as it relates to the use of computers, is no different than proper behavior in all other aspects of West Hardin C.C.I.S.D. activities. All users are expected to use the computers and computer networks in a responsible, ethical, and polite manner. This document is intended to clarify those expectations as they apply to computer and network usage and is consistent with District Policy.

DEFINITION OF DISTRICT TECHNOLOGY RESOURCES

The District's computer systems and networks are any configuration of hardware and software. The systems and networks include all of the computer hardware, operating system software, application software, stored text, and data files. This includes electronic mail, local databases, externally accessed databases (such as the Internet), CD-ROM, optical media, clip art, digital images, digitized information, communications technologies, and new technologies as they become available. The District reserves the right to monitor all technology resource activity.

ACCEPTABLE USE

The District's technology resources will be used only for learning, teaching and administrative purposes consistent with the District's mission and goals. Commercial use of the District's system is strictly prohibited.

The District will make training available to all users in the proper use of the system and will make copies of acceptable use guidelines available to all users. All training in the use of the District's system will emphasize the ethical use of this resource.

Software or external data may not be placed on any computer, whether stand-alone or networked to the District's system, without permission from the Technology Director or Network Administrator.

Other issues applicable to acceptable use are:

1. **Copyright:** All users are expected to follow existing copyright laws, copies of which may be found in the library.
2. **Supervision and permission:** A staff member only allows student use of the computers and computer network when supervised or granted permission.
3. **Attempting to log on or logging on to a computer or small system by using another's password is prohibited:** Assisting others in violating this rule by sharing information or passwords is unacceptable.
4. **Improper use of any computer or the network is prohibited. This includes the following:**
 - o Submitting, publishing or displaying any defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented, or threatening materials or messages either public or private.
 - o Using the network for financial gain, political or commercial activity
 - o Attempting to or harming equipment, materials or data
 - o Attempting to or sending anonymous messages of any kind
 - o Using the network to access inappropriate, obscene, or pornographic material
 - o Knowingly placing a computer virus on a computer or the network
 - o Using the network to provide addresses or other personal information that others may use inappropriately
 - o Accessing of information resources, files and documents of another user without authorization

SYSTEM ACCESS

Access to the District's network systems will be governed as follows:

1. Students will have access to the District's resources for class assignments and research with their teacher's permission and supervision.
2. Teachers with accounts will be required to maintain password confidentiality by not sharing the password with anyone.
3. District employees will be granted access to the District's system.
4. Any system user identified as a security risk of having violated District Acceptable Use Guidelines may be denied access to the District's system. Other consequences may also be assigned.
5. Any system user having been denied access rights may be reinstated with a limited access account to reduce the level of security risk to the system. Limits on this type of account may include time limitations, station access limitations, file access restrictions, and a revocation of Internet access privileges.

CAMPUS LEVEL RESPONSIBILITIES

The campus principal or designee will:

1. Be responsible for disseminating, collecting signed permission forms, and enforcing the District Acceptable Use Guidelines for the District's system at the campus level.
2. Ensure that employees supervising students who use the District's systems provide information emphasizing the appropriate and ethical use of this resource.

INDIVIDUAL USER RESPONSIBILITIES

The following standards will apply to all users of the District's computer network systems:

1. The Individual in whose name a system account is issued will be responsible at all times for its proper use.
2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by district guidelines,
3. System users may not use another person's system account,
4. System users are asked to delete electronic mail or outdated files on a regular basis.
5. System users will be responsible for the care and maintenance of their systems. Maintenance issues should be reported to the Network Administrator.
6. System users will be responsible for following all copyright laws.

VANDALISM PROHIBITED

Any attempt to harm or destroy District equipment or materials, data of another user of the District's system, or any of the agencies or other networks to which the District has access is prohibited. Intentional attempts to degrade or disrupt system performance may be viewed as violations of district guidelines and, possibly, as criminal activity under applicable state and federal laws, including the Texas Penal Code, Computer Crimes, Chapter 33. This includes, but is not limited to, the uploading or creating of computer viruses, system break-in utilities, or system hacking programs.

Vandalism as defined above will result in the cancellation of system use privileges and possible prosecution. The party will be responsible for restitution of costs associated with system restoration, hardware, or software costs.

FORGERY PROHIBITED

Forgery or attempted forgery of electronic messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users or deliberate interference with the ability of other system users to send/receive electronic mail is prohibited.

INFORMATION CONTENT/THIRD PARTY SUPPLIED INFORMATION

System users and parents of students with access to the District's system should be aware that use of the system may inadvertently provide access to other electronic communications systems outside the District's networks that may contain inaccurate and/or objectionable material. The District will maintain an Internet filtering software package to attempt to minimize the access to objectionable and inappropriate information. Any attempt to circumvent the filtering software will be viewed as an attempt to disrupt the system. Subject to staff supervision, Internet filters may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Technology Coordinator.

A student bringing prohibited materials into the school's electronic environment will be subject to a suspension and/or a revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Student Code of Conduct. An employee knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies. This could result in loss of credit for students or termination of employment for employees.

ELECTRONIC MAIL, CHAT ROOMS AND NETWORK FOLDERS

Students will be provided filtered email accounts at the teacher's request. This will be the only email account that students will be allowed to access while at school. Chat rooms will not be allowed unless requested by a teacher for a specific project.

Staff will be provided an email account through Region 5 Educational Service Center. In addition, staff will utilize West Hardin C.C.I.S.D.'s local email network, Quickmail, on a daily basis at work as a primary tool for communications. The district will rely on this environment to communicate information and all staff will be responsible for checking and reading messages daily. Quickmail is to be used for school business only.

West Hardin C.C.I.S.D. reserves the right to review any material on student and staff email accounts or network folders. Network administrators may review files and communications to maintain system integrity and ensure that users are using the system responsibly. Users should not expect that files stored on district servers will always be private. Within reason, freedom of speech and access to information will be honored.

NETWORK ETIQUETTE

System users are expected to observe the following network etiquette (also known as netiquette):

1. Use appropriate language: swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language is prohibited.
2. Pretending to be someone else when sending or receiving messages is prohibited.
3. Submitting, publishing or displaying any defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented, or threatening materials or messages either public or private.
4. Revealing such personal information as addresses or phone numbers of users or others is prohibited.
5. Using the network in such a way that would disrupt the use of the network by other users is prohibited.
6. Be polite. For example, messages typed in capital letters are the computer equivalent of shouting and are considered rude.

SUSPENSION/REVOCAION OF SYSTEM USER ACCOUNT

The District will suspend or revoke a system user's access to the District's system upon violation of District policy and/or administrative regulations regarding acceptable use.

Termination of an employee's account or of a student's access will be effective on the date the principal or designee receives notice of user withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

CONSEQUENCES OF IMPROPER USE

Improper or unethical use may result in disciplinary actions consistent with the existing Student Discipline Policy and, if appropriate, the Texas Penal Code, Computer Crimes, Chapter 33, or other state and federal laws. This may also require restitution for costs associated with system restoration, hardware, or software costs.

DISCLAIMER

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether expressed or implied, including, without limitation, those of fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District uses a variety of vendor-supplied hardware and software. Therefore, the District does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the user's requirements. Neither does the District warrant that the system will be uninterrupted or error-free, nor that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third party individuals in the system are those of the providers and not necessarily the District.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's computer systems and networks.

TERM

This policy is binding for the duration of the student's enrollment and staff's employment in West Hardin C.C.I.S.D.