

Hamlin Independent School District
Acceptable Use Guidelines and Regulations
for
Internet and Other Electronic Communications Systems

OVERSIGHT

The Superintendent or designee will oversee the District's electronic communications systems.

TRAINING

The District will provide training in proper use of the systems and will provide all users with copies of acceptable use guidelines. All training in the use of the District's systems will emphasize the ethical use of these resources.

CONSENT
REQUIREMENTS

Copyrighted software or data may not be placed on any system connected to a District system without permission from the holder of the copyright. Only the owners or individual(s) the owner specifically authorize(s) may upload copyrighted material to the system.

No original work created by any District student or employee will be posted on a web page under the District's control unless the District has received written consent from the student (and the student's parent) or employee who created the work.

No personally identifiable information about a District student will be posted on a web page under the District's control unless the District has received written consent from the student's parent. An exception may be made for "directory information" as allowed by the Family Education Records Privacy Act and District policy.

SYSTEM ACCESS

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

1. As appropriate and with the written approval of the immediate supervisor, District employees will be granted access to the District's systems.

2. Students in grades PK - 8 will be granted access to the District's system by their teachers, as appropriate. Students in grades 9 - 12 will be assigned individual accounts.
3. A teacher may apply for a class account and in doing so will be ultimately responsible for use of the account.
4. The District will require that all passwords be changed every semester or trimester, if applicable.
5. Any system user identified as a security risk or as having violated District and/or campus computer use guidelines may be denied access to the District's system.

TECHNOLOGY
COORDINATOR
RESPONSIBILITIES

The technology coordinator for the District's electronic communications systems (or campus designee) will

1. Be responsible for disseminating and enforcing applicable District policies and acceptable use guidelines for the District's systems.
2. Ensure that all users of the District's system complete and sign an agreement to abide by District policies and administrative regulations regarding such use. All such agreements will be maintained on file in the principal's or supervisor's office.
3. Ensure that employees supervising students who use the District's systems provide training emphasizing the appropriate use of this resource.
4. Ensure that all software loaded on computers in the District is consistent with District standards and is properly licensed.
5. Be authorized to monitor or examine all system activities, including electronic mail transmissions, as deemed appropriate to ensure proper use of the system.
6. Be authorized to establish a retention schedule for messages on any electronic bulletin board and to remove messages posted locally that are deemed to be inappropriate.

7. Set limits for data storage within the District's systems as needed.

INDIVIDUAL USER RESPONSIBILITIES

The following standards will apply to all users of the District's electronic information/communications systems:

ON-LINE CONDUCT

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 policy or guidelines.
3. System users may not use another person's system account without written permission from the campus administrator or District coordinator, as appropriate.
4. Students may not distribute personal information about themselves or others by means of the electronic communication system.
5. System users must purge electronic mail in accordance with established retention guidelines.
6. System users may not redistribute copyrighted programs or data except with the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with applicable copyright laws, District policy, and administrative regulations.
7. System users may upload public domain programs to the system. System users may also download public domain programs for their own use or may noncommercially redistribute a public domain program. System users are responsible for determining whether a program is in the public domain.
8. System users may not send or post messages that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, disrespectful of others, or illegal.

9. System users may not purposefully access materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, disrespectful of others, or illegal.
10. System users should be mindful that use of school-related electronic mail addresses might cause some recipients or other readers of that mail to assume they represent the District or school, whether or not that was the user's intention.
11. System users may not waste District resources related to the electronic communications system.
12. System users may not gain unauthorized access to resources or information.
13. While at school or when using District equipment or systems, students may not access any e-mail account except that created for them by Hamlin I.S.D.

VANDALISM PROHIBITED

Any malicious attempt to harm or destroy District equipment or data or data of another user of the District's system, or any of the agencies or other networks that are connected to the Internet, is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of District policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above will result in the cancellation of system use privileges and will require restitution for costs associated with system restoration, as well as other appropriate consequences.

FORGERY PROHIBITED

Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users, deliberate interference with the ability of other system users to send/receive electronic mail, or the use of another person's user ID and/or password, 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 provide access to other electronic communications systems in the global electronic network that may contain inaccurate, pornographic, and/or otherwise objectionable material.

A student who gains access to such material is expected to discontinue the access as quickly as possible and to report the incident to the supervising teacher.

A student knowingly bringing prohibited materials into the school's electronic environment will be subject to suspension of access and/or 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.

PARTICIPATION IN
CHAT ROOMS AND
NEWSGROUPS

Students are prohibited from participating in any chat room or newsgroup accessed on the Internet. Employees may participate in newsgroups, in accordance with District policies and regulations, but may not participate in chat rooms.

DEVELOPMENT
OF WEB PAGES

Any web page developed by students or employees on District systems must have prior approval by the appropriate administrator.

NETWORK
ETIQUETTE

System users are expected to observe the following network etiquette:

1. Be polite; messages typed in capital letters are the computer equivalent of shouting and are considered rude.
2. Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited.
3. Pretending to be someone else when sending/receiving messages is considered inappropriate.
4. Transmitting obscene messages or pictures is prohibited.
5. Using the network in such a way that would disrupt the use of the network by other users is prohibited.

TERMINATION/ REVOCATION OF SYSTEM USER ACCOUNT

Termination of an employee's or a student's access for violation of District policies or regulations will be effective on the date the principal or District coordinator receives notice of student withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

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 merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. 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 system user's requirements, or that the system will be uninterrupted or error-free, or 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 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 electronic communications system.

HAMLIN INDEPENDENT SCHOOL DISTRICT
EMPLOYEE AGREEMENT FOR ACCEPTABLE USE
of the
ELECTRONIC COMMUNICATIONS SYSTEM

You are being given access to the HISD Electronic Communications System. Through this system, you will be able to communicate with other schools, colleges, organizations, and people around the world through the Internet and other electronic information systems/networks. You will have access to hundreds of databases, libraries, and computer services all over the world.

With this opportunity comes responsibility. It is important that you read the District policy, administrative regulations, and agreement form and ask questions if you need help in understanding them. Inappropriate system use will result in the loss of the privilege of using this educational and administrative tool.

Please note that the Internet is a network of many types of communication and information networks. It is possible that you may run across some pornographic or otherwise objectionable material. While the District will take reasonable steps to restrict access to such material, it is not possible to absolutely prevent such access. It will be your responsibility to follow the rules for appropriate use.

Rules for Appropriate Use

- . The account is to be used mainly for educational purposes, but some limited personal use is permitted.
- . You will be held responsible at all times for the proper use of your account, and the District may suspend or revoke your access if you violate the rules.
- . Remember that people who receive e-mail from you with a school address might think your message represents the school's point of view.
- . If you should unintentionally access material that is pornographic or otherwise objectionable, you must immediately discontinue the access and report the incident to your supervisor.