Vidor Independent School District
Electronic Communications System Policy and Administrative Regulations

Electronic Communication and Data Management

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

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

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

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

System Access

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

1. With the approval of the immediate supervisor, District employees will be granted access to the District's system.
2. The District will require that all passwords be changed.
3. A teacher may apply for a class account and, in doing so, will be ultimately responsible for use of the account. Teachers with accounts will be required to maintain password confidentiality by not sharing the password with students or others.
4. Students completing required course work on the system will have first priority for use of District equipment after school hours.
5. Any system user identified as a security risk or having violated District and/or campus computer-use-guidelines may be denied access to the District's system.

Campus-Level Coordinator Responsibilities

As the campus-level coordinator of the electronic communications system, the principal or designee will:

1. Be responsible for disseminating and enforcing applicable District policies and acceptable use guidelines for the District's system at the campus level.
2. Ensure that all users of the District's system complete and sign an agreement to abide by District's policies and administrative regulations regarding such use. All such agreements will be maintained on file in the technology office.
3. Ensure that employees supervising students who use the District's system provide training emphasizing the appropriate use of this resource.
4. Be authorized to monitor or examine all system activities, including electronic mail transmissions, as deemed appropriate to ensure proper use of the system.
5. 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.
6. Set limits for disk utilization on the system, as needed.

Individual User Responsibilities On-Line Conduct

The following standards will apply to all users of the District's electronic information / communications 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 policy.
3. System users may not use another person's system account without written permission from the campus administrator or District coordinator, as appropriate.
4. System users must purge electronic mail in accordance with established retention guidelines.
5. System users may redistribute copyrighted programs or data only 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.

6. System users may upload public domain programs to the system. System users may also download public domain programs for their own use or may non-commercially redistribute a public domain program. System users are responsible for determining whether a program is in the public domain.

Vandalism Prohibited

Any malicious attempt to harm or destroy District equipment or materials, data or 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 may be viewed as violations of District policy and administrative regulations and, possibly, as criminal activity under applicable state and federal laws. This 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, hardware, or software costs.

Forgery or attempted forgery of electronic mail 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.

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 and/or objectionable material.

A student knowingly 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.

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. Revealing personal addresses or phone numbers of the user or others is prohibited.
6. Using the network in such a way that would disrupt the use of the network by others is prohibited.

Termination/Revocation of System User Account

The District may 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 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 express 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 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.