PEIMS

The principal of each campus is responsible for reviewing his or her respective Campus Data Reports for data integrity and must have a system of internal controls in place to maintain the ability to reproduce, for audit purposes, all required documentation. Reports from the Texas Education Agency (TEA), which reflect Public Education Information Management System (PEIMS) data should be compared to locally produced reports for reasonableness and accuracy. The principal's signature on PEIMS signoff sheets and attendance reports affirms that the principal has checked, or caused to be checked, the accuracy and authenticity of the PEIMS data.

SYSTEM ACCESS

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

1. District employees will be granted access to the District's system [see CQ (EXHIBIT A)].
2. Students will be given access to the District's system only upon receipt of written parental approval [see CQ (EXHIBIT B)].
3. A teacher may apply for a class account and in doing so will be ultimately responsible for use of the account.
4. 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.

RESPONSIBILITIES OF TECHNOLOGY DEPARTMENTS

The technology departments of the District will:

1. Be responsible for updating the acceptable use guidelines for the District's electronic network.
2. Provide training in proper use of the system. Training in the use of the District's system will emphasize the ethical use of the District's network and information security over wireless networks.
3. Set limits for data storage within the District's network as needed.

RESPONSIBILITY OF CAMPUSES/ DEPARTMENTS

Campus administrators and department supervisors will:

1. Be responsible for disseminating and enforcing (with the help of personnel from the MIS and Technology Services departments) applicable District policies and acceptable use guidelines for the District's system.

2. Ensure that all student users of the District's system and their parent/guardian complete and sign an agreement to abide by District policies and administrative regulations regarding acceptable use [see CQ (EXHIBIT B)]. All such agreements will be maintained on file in the principal's office.
3. Ensure that all employees using the District's system complete and sign an agreement [CQ (EXHIBIT A)] to abide by District policies and administrative regulations regarding acceptable use. All such agreements will be sent to the Personnel Department. Supervisors of District employees must make sure that all employees have signed the agreement before access is allowed.
4. Ensure that employees supervising students who use the District's system provide training emphasizing the appropriate use of this resource.
5. Ensure that all software loaded on computers in the District is consistent with District standards and is properly licensed.
6. Ensure that employees who check-out equipment sign the "Custody Receipt Form." [See CMB (R) and CLD (R)]

RESPONSIBILITIES OF RISK MANAGEMENT OFFICE

1. Investigate equipment losses to determine fiduciary responsibility.
2. Coordinate possible financial reimbursements to the District.

RESPONSIBILITIES OF THE USER

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

1. System users are responsible for following the rules established by the District for acceptable use. [CQ (EXHIBIT)]
2. 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.
3. System users are responsible for following all copyright laws and regulations.

4. System users shall not use district system or equipment for financial gain, political or commercial activity, or accessing inappropriate content.
5. System users who check out equipment must sign and abide by the "Custody Receipt Form." [See CMB (R) and CLD (R)]
6. Confidential information, to include student or employee data, will be encrypted prior to being sent across wireless connections.

DEVELOPMENT OF WEB PAGES

Each campus/department will be responsible for maintaining a web- site. Each campus/department will:

1. Identify a web page coordinator for the campus/department. The web page coordinator will be responsible for designing the main site web page and will coordinate the upload-ing/screening of web pages developed by other personnel in the campus/department. The principal/director will act as the final decision maker for web content.
2. The web page coordinator will attend specialized training offered by the District in web page development and maintenance.
3. All District-owned or District-sponsored web pages should reside on the NEISD web server.
4. Campus and central office department web pages will be updated on a regular basis to keep information current.
5. Links from web pages on the District web server will not lead to commercial web sites that advertise a product or service unless approved by the Superintendent or his de-signee. At no time will such links be for personal gain.

ACCESS TO E-MAIL AND PRIVACY

1. All users shall understand that the District cannot guarantee the privacy or confidentiality of electronic documents and any e-mail messages that are confidential as a matter of law should not be communicated using email.
2. The District reserves the right to access e-mail to engage in routine computer maintenance and housekeeping, to carry out internal investigations, to prepare responses to requests for public records, or to disclose messages, date, or files to law enforcement authorities.

3. Messages sent as electronic mail should meet the same standards for distribution as if they were tangible documents or instruments. As with all records maintained by the District and to the extent required by law, files saved in the District's system, including e-mail, may be subject to release with a public records disclosure request.

VANDALISM PROHIBITED

Any malicious 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 that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance shall be viewed as violations of District policy and administrative regulations and, possibly, as 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 network 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 or 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

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.

1. 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.

2. 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.

3. An employee knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies.

CONSENT REQUIREMENTS

1. Copyrighted software or data may not be placed on any system without permission of the copyrighted holder or designee. Only the owner(s) or individual(s) the owner specifically authorizes may upload copyrighted material to the system.
2. No original work created by any District student 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) who has created the work.
3. 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.

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 department supervisor receives notice of student withdrawal or of revocation of network 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 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.