PEIMS

The Superintendent will designate a central administrator to oversee the District's Public Education Information Management System (PEIMS).

PEIMS RESPONSIBILITIES

The central office administrator, designated to oversee PEIMS will develop and disseminate a PEIMS accountability system for the District. The accountability system will include procedures for monitoring and validating the accuracy of PEIMS data throughout the school year.

PRINCIPAL

The principal is responsible for the following:

1. Designating an administrator to coordinate the gathering, inputting, and verification of PEIMS data.
2. Designating personnel responsible for data entry.
3. Submitting the "designation form" to the Chief Financial Officer. [See CQ (REG) (EXHIBIT A)]
4. Monitoring the fulfillment of assigned duties related to PEIMS accountability.
5. Including assessment of PEIMS-related duties in the evaluation of the PEIMS administrator and data entry personnel.

CAMPUS-BASED PEIMS ADMINISTRATOR

The campus-based PEIMS administrator is responsible for the following:

1. Participating in training as needed to perform PEIMS-related duties.
2. Coordinating the gathering and inputting of all data required for PEIMS.
3. Ensuring that supporting documentation is maintained for every data entry for use in verification and correction purposes.
4. Assuming responsibility for edits, reports, and verification checks on data each six weeks to ensure the accuracy of information.
5. Printing and distributing edits and reports to appropriate staff for verification and correction.
6. Assuming responsibility for ensuring that corrections and verifications are made as needed to perform PEIMS-related duties.
7. Submitting a copy of signed verification log to the Chief Financial Officer at the end of each six weeks on or before designated deadlines. [See CQ (REG) (EXHIBIT B)]
8. Being available to complete edits, verifications, and corrections for final submission of the District's file to TEA in the summer.

PEIMS DATA ENTRY PERSONNEL

The PEIMS data entry personnel are responsible for the following:

1. Participating in training as needed to perform PEIMS-related duties.

2. Inputting all data required for PEIMS submission in an accurate and timely manner.

3. Keeping campus-based PEIMS administrator informed of problems or concerns related to PEIMS data, edits, or verifications.

4. Printing and reviewing edits, reports and verification checks on PEIMS data each six weeks to verify the accuracy of the information.

5. Submitting verified/corrected edits/reports to campus-based administrator at the end of each six weeks.

6. Signing six-week PEIMS verification log as documentation of task completion. [See CQ (REG) (EXHIBIT B)]

7. Being available to complete edits, verifications, and corrections for final submission of the District's file to TEA in the summer.

ELECTRONIC NETWORK AND COMMUNICATION SYSTEM

The Assistant Superintendent for Curriculum and Instruction or designee will manage and oversee the District's electronic network and communication systems. The Assistant Superintendent for Curriculum and Instruction or designee will provide training in proper use of the system and will provide all users with copies of District-approved acceptable use guidelines. All training will emphasize the ethical use of these electronic resources.

DEFINITION OF SYSTEM

The District's computer systems and networks (system) are any configuration of-hardware and software. The system includes but is not limited to the following:

1. Telephones, pagers and voicemail facilities;

2. Electronic mail (e-mail) accounts;

3. Fax machines;

4. Servers;

5. Computer hardware and peripherals;

6. Software including operating system software and application software;

7. Digitized information including stored text, data files, electronic mail, digital images and audio files;

8. Internally accessed databases or tools;

9. External accessed databases (such as the Internet); and

10. New technologies as they become available.

COPYRIGHT AND CONSENT REQUIREMENTS

Copyrighted software or data may not be placed on any District system without permission from the holder of the copyright and the Assistant Superintendent for Curriculum and Instruction. Unauthorized use of copyrighted material is prohibited as specified in Board policy.

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. [See CQ (REG) (EXHIBIT C)]

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 Rights and Privacy Act (FERPA) and District policy. [See CQ (REG) (EXHIBIT C) and Board policy FL]

SYSTEM ACCESS

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

1. All District employees will be granted access to the District's system with the approval of the principal or departmental supervisor or designee.
2. Students in secondary grades will be assigned individual access accounts, as appropriate. Students may be allowed to use the local network with campus permission, but may only use the Internet with parent permission. Student Internet access will be under the direction and guidance of a teacher or staff member.
3. All non-employee/non-student users must obtain approval from the principal or departmental supervisor or designee to gain access to the District's system.
4. The District's system is subject to internal monitoring by designated staff at any time to ensure appropriate use. All electronic files, including electronic mail messages shall not be considered confidential or private unless protected by law.
5. Internet access to personal e-mail accounts is not allowed.
6. Any 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.

DISTRICT-LEVEL RESPONSIBILITIES

The Assistant Superintendent for Curriculum and Instruction or designee will:

1. Review and update the District-approved acceptable use guidelines as needed to comply with legal statutes and local practices. Any necessary revisions will be presented to the Superintendent's Cabinet for approval.
2. Ensure that all software loaded on computers is consistent with District standards and is properly licensed.

3. Plan, schedule and document delivery of required training to all District-level employees.

4. Establish, communicate, and monitor the limits for data storage/retention.

CAMPUS- AND DEPARTMENTAL-LEVEL RESPONSIBILITIES

The principal/departmental administrator or designee will:

1. Be responsible for disseminating and enforcing applicable District policies and acceptable use guidelines for the District's system.

2. Ensure that all individual 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 departmental supervisor's office.

3. Ensure that employees supervising students who use the District's system provide training emphasizing the appropriate use of this resource.

4. Monitor and examine all system users to ensure appropriate and ethical use of the District's systems.

INDIVIDUAL USER RESPONSIBILITIES

The individual user shall read, agree to abide by, and sign the District-approved acceptable use guidelines. The following standards will apply to all users of the District's system:

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 administrative regulation.

3. System users may not use another person's system account.

4. System users may not send or post messages that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

5. System users may not purposefully access materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

6. System users may not use District electronic mail to conduct political lobbying. (See Exhibit C, page 5 of 8 at “Political Lobbying”)

7. System users may not use District electronic mail to distribute or forward chain letters, or other annoying or unnecessary messages. (See Exhibit C, page 5 of 8 at “Junk Mail/Chain Letters”)

8. System users may not use District electronic mail to promote activities or events for individuals or organizations not directly affiliated with or sanctioned by the District. Permission to distribute information regarding

these activities or events must be approved by appropriate campus/department/District administrator.

9. System users may not waste District resources related to the electronic communications system.

10. System users may not gain unauthorized access to resources or information.

11. System users must always respect copyrights and trademarks of third-parties and their ownership claims in images, text, video and audio material, software, information and inventions. The copy, use or transfer of others' materials without appropriate authorization is not allowed.

12. 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.

13. System users may not redistribute or forward confidential information (i.e. educational records, directory information, personnel records, etc.) without proper authorization. Confidential information should never be transmitted, redistributed or forwarded to outside individuals who are not expressly authorized to receive the information. Revealing such personal information as home addresses or phone numbers of users or others is prohibited.

VANDALISM PROHIBITED

Any malicious attempt to harm or destroy District equipment, materials or data, or the malicious attempt to harm or destroy 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. 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 is prohibited and will result in the cancellation of system use privileges. System users committing vandalism will be required to provide restitution for costs associated with system restoration and may be subject to other appropriate consequences. [See DH, FN series, and FO series in Board Policy and the Board-Approved *Discipline Management Plan and the Student Code of Conduct*]

FORGERY/ IMPERSONATION/ PLAGIARISM 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.

Fraudulently altering or copying documents or files authored by another individual or assuming the identity of another individual 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 and/or 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 who knowingly brings 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 Board-approved *Discipline Management Plan and Student Code of Conduct*.

An employee who knowingly brings prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies. [See Board policy DH]

PARTICIPATION IN CHAT ROOMS AND NEWSGROUPS

Students and employees are restricted from participating in any chat room or newsgroup accessed on the Internet.

STUDENT EMAIL ACCOUNTS

The following will apply to student email usage:

1. No student will be assigned an individual email account or password.
2. Students are prohibited from accessing personal email accounts using the District's system.
3. As appropriate and with written approval of the appropriate District personnel in the Curriculum Department and in the Technology Department, project email accounts will be granted for specific educational activities. [See CQ (REG) (EXHIBIT D)]

DEVELOPMENT OF WEB PAGES

The purpose of District web sites is to promote communication of campus, department, and District activities and provide relevant information. All campus and departmental sites must be hosted on the District web server.

DISTRICT-LEVEL RESPONSIBILITIES

The Assistant Superintendent for Curriculum and Instruction or designee will provide training, assistance, and resources to support campuses and departments in their efforts to meet District web site guidelines.

CAMPUS AND DEPARTMENT RESPONSIBILITIES

The principal/departmental supervisor or designee will be responsible for approving the content and maintenance schedule for the web sites under their supervision prior to publishing. [See CQ (REG) (EXHIBIT E)]

The campus/departmental designee will be responsible for the development and maintenance of the campus/department web site.

WEB PAGE CONTENTS

Web pages hosted on the District web server and hyperlinks from these web pages must not contain information that is in violation of (or promotes the violation of) any District policy or regulation nor any local, state, or federal regulation or law.

Web pages that contain time-sensitive information, such as calendars, school events, staff information, etc., must be kept current.

Web pages must be checked at least every month to ensure that links are current and operable.

EXTERNAL LINKS

In all cases where an external link (link to a site not hosted on the District web server) is used on a school's web site, the following disclaimer statement must be present on the school's main navigation page:

Northwest ISD is not responsible for the contents on external sites or servers.

Educational links are allowed if they are reviewed for educational appropriateness by the Assistant Superintendent for Curriculum and Instruction or designee. External links to sites that are not accessible inside the network through the filtering system are prohibited.

Links to non-official Northwest ISD related sites that are hosted on remote/external (non-District) web servers are prohibited unless prior authorization to such action has been obtained from the appropriate District personnel.

COMMERCIALISM

Commercial advertising shall be prohibited on all campus and District web pages.

EMPLOYEE WEB PAGES

Employee web pages must meet the following criteria:

1. All employee web pages must include the date it is updated.
2. "Guestbooks," "chat areas," "message boards" or similar links are prohibited.
3. When a District system for posting individual web pages is made available, all classroom information must be moved to the District system. Links to staff or volunteer pages not hosted on an approved site, or the District web server, are prohibited.
4. Northwest ISD email addresses may be listed on a District web site in accordance with District/campus procedures.
5. Personal information about District employees and parent volunteers will not be disclosed without the approval of the individual and the principal/departmental supervisor and will be in accordance with District/campus procedures. Non-District email addresses, non-District mailing addresses, and non-District phone numbers will not be disclosed on District/campus web sites.

6. Pictures and names of employees and parent volunteers are allowed with their approval.

STUDENT INFORMATION

The following web page guidelines apply to student information:

1. No personal student home pages are permitted on a District web site. Links to personal student home pages from a District web site are not permitted.

2. Student work is permitted on the campus web site if the appropriate parental permission has been obtained. [See CQ (REG) (EXHIBIT F)]

3. Student pictures and names are permitted if the parent-selected privacy code allows such release and in the case of photographs, specific parental permission has been granted. [See CQ (REG) (EXHIBIT F)]

   Guidelines for use of names on a District web page **if** appropriate permissions are obtained from parent/guardian will be as follows:

   Elementary: Student's picture or work with first name only.

   Secondary: Student's picture or work with first name, or first name and last initial only.

4. No other personal information about a student is allowed such as email address, phone number, home address, and birth date.

SECURITY

Knowledge of inappropriate material or a security problem on the Network/Internet should be reported immediately to the Director of Technology. Impersonation of a system administrator, District employee, student, or an individual other than the user will result in revocation of the user’s access to the Network/Internet.

Any user identified as having had access privileges revoked or denied on another computer system may be denied access to the District’s Network/Internet.

CONSEQUENCES OF AGREEMENT VIOLATION

Any attempt to violate the provisions of this agreement may result in revocation of the user’s access to the Computer/Network/Internet, regardless of the success or failure of the attempt. In addition, appropriate disciplinary measures and/or legal action will be taken based on whether the user is a student, employee or other person.

TERMINATION/ REVOCATION OFSYSTEM USER ACCOUNT

Termination of an employee's or a student's access for violation of District policies or administrative 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.

WARNING

Sites accessible via the Network/Internet may contain material that is illegal, defamatory, inaccurate or controversial. Each District computer with Internet access has filtering software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children’s Internet Protection Act. The District makes every effort to limit access to objectionable material; however, controlling all such materials on the Network/Internet is impossible, even with filtering in place. With global access to computers and people, a risk exists that students may access material that may not be of educational value in the school setting. The District’s Internet connection is the only system to be used in schools. No commercial Internet accounts may be used.

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.