

Appendix A

Policy for Acceptable Use of Plano Independent School District Technology Resources

The Plano 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 Plano 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, through their use, 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. Plano ISD 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 technology, is no different than proper behavior in all other aspects of Plano ISD activities. All users are expected to use the technology and networks in a responsible, ethical, and polite manner. This appendix is intended to clarify those expectations as they apply to technology and network usage and consists of District Policy CQ (Legal, Local, Regulations and Exhibits).

Plano ISD
043910

ELECTRONIC COMMUNICATION AND DATA
MANAGEMENT

CQ
(LEGAL)

PEIMS

The District shall participate in the Public Education Information Management System (PEIMS) and through that system shall provide information required for the administration of the Foundation School Program and of other appropriate provisions of the Education Code. The PEIMS data standards, established by the Commissioner of Education, shall be used by the District to submit information. *Education Code 42.006; 19 TAC 61.1025*

CHILDREN'S

Under the Children's Internet Protection Act (CIPA), the District



INTERNET
PROTECTION ACT

must, as a prerequisite to receiving universal service discount rates, implement certain Internet safety measures and submit certification to the Federal Communications Commission (FCC). *47 U.S.C. 254* [See UNIVERSAL SERVICE DISCOUNTS, below, for details]

Districts that do not receive universal service discounts but do receive funding under the Technology for Education Act of 1994 (Title III of the Elementary and Secondary Education Act [ESEA]) must, as a prerequisite to receiving these funds, implement certain Internet safety measures and submit certification to the Department of Education (DOE). *20 U.S.C. 7001* [See ESEA FUNDING, below, for details]

DEFINITIONS

"Harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

47 U.S.C. 254(h)(7)(G), 20 U.S.C. 7001(a)(5)(F)

"Technology protection measure" means a specific technology that blocks or filters Internet access. *47 U.S.C. 254(h)(7)*

"Universal service" means telecommunications services including Internet access, Internet services, and internal connection services and other services that are identified by the FCC as eligible for federal universal service support mechanisms. *47 U.S.C. 254(c)(3), (h)(5)(A)(ii)*

UNIVERSAL
SERVICE
DISCOUNTS

An elementary or secondary school having computers with Internet access may not receive universal service discount rates unless the District implements an Internet safety policy, submits certifications to the FCC, and ensures the use of computers with Internet access in accordance with the certifications. *47 U.S.C. 254(h)(5)(A), (I); 47 CFR 54.520*

INTERNET
SAFETY POLICY

The District shall adopt and implement an Internet safety policy that addresses:



1. Access by minors to inappropriate matter on the Internet and the World Wide Web;
2. The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
3. Unauthorized access, including "hacking," and other unlawful activities by minors on-line;
4. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors; and
5. Measures designed to restrict minors' access to materials harmful to minors.

47 U.S.C. 254(l)

PUBLIC HEARING

The District shall provide reasonable public notice and hold at least one public hearing or meeting to address the proposed Internet safety policy. *47 U.S.C. 254(h)(5)(A), (l)(1)*

INAPPROPRIATE FOR MINORS

A determination regarding what matter is inappropriate for minors shall be made by the Board or designee. *47 U.S.C. 254(l)(2)*

TECHNOLOGY PROTECTION MEASURE

In accordance with the appropriate certification, the District shall operate a technology protection measure that protects minors against access to visual depictions that are obscene, child pornography, or harmful to minors; and protects adults against access to visual depictions that are obscene or child pornography. *47 U.S.C. 254(h)(5)(B), (C)*

MONITORED USE

In accordance with the appropriate certification, the District shall monitor the on-line activities of minors. *47 U.S.C. 254(h)(5)(B)*

CERTIFICATIONS TO THE FCC

To be eligible for universal service discount rates, the District shall certify to the FCC, in the manner prescribed at 47 CFR 54.520, that:

1. An Internet safety policy has been adopted and implemented.
2. With respect to use by minors, the District is enforcing the Internet safety policy and operating a technology protection measure during any use of the computers.
3. With respect to use by adults, the District is enforcing an Internet safety policy and operating a technology protection measure during any use of the computers,



except that an administrator, supervisor, or other person authorized by the District may disable the technology protection measure during use by an adult to enable access for bona fide research or other lawful purpose.

47 U.S.C. 254(h)(5); 47 CFR 54.520

ESEA FUNDING

Federal funds made available under the Technology for Education Act of 1994 (Title III of the Elementary and Secondary Education Act [ESEA]) for an elementary or secondary school that does not receive universal service discount rates may not be used to purchase computers used to access the Internet, or to pay for direct costs associated with accessing the Internet unless the District:

MINORS

1. Has in place a policy of Internet safety for minors that includes the operation of a technology protection measure that protects against access to visual depictions that are obscene, child pornography, or harmful to minors and enforces the operation of the technology protection measure during any use by minors of its computers with Internet access; and

ADULTS

2. Has in place a policy of Internet safety that includes the operation of a technology protection measure that protects against access to visual depictions that are obscene or child pornography; and enforces the operation of the technology protection measure during any use of its computers with Internet access.

The District may disable the technology protection measure to enable access to bona fide research or for another lawful purpose.

CERTIFICATION TO DOE

The District shall certify its compliance with these requirements to the Department of Education as part of the annual application process for each program funding year under the ESEA.

20 U.S.C. 7001(a)

TRANSFER OF EQUIPMENT TO STUDENTS

The District may transfer to a student enrolled in the District:

1. Any data processing equipment donated to the District, including equipment donated by a private donor, a state eleemosynary institution, or a state agency under Government Code 2175.126;
2. Any equipment purchased by the District; and



3. Any surplus or salvage equipment owned by the District.

Education Code 32.102(a)

Before transferring data processing equipment to a student, the District must:

1. Adopt rules governing transfers, including provisions for technical assistance to the student by the District;
2. Determine that the transfer serves a public purpose and benefits the District; and
3. Remove from the equipment any offensive, confidential, or proprietary information, as determined by the District.

Education Code 32.104

DONATIONS

The District may accept:

1. Donations of data processing equipment for transfer to students; and
2. Gifts, grants, or donations of money or services to purchase, refurbish, or repair data processing equipment.

Education Code 32.102(b)

USE OF PUBLIC FUNDS

The District may spend public funds to:

1. Purchase, refurbish, or repair any data processing equipment transferred to a student; and
2. Store, transport, or transfer data processing equipment under this policy.

Education Code 32.105

ELIGIBILITY

A student is eligible to receive data processing equipment under this policy only if the student does not otherwise have home access to data processing equipment, as determined by the District. The District shall give preference to educationally disadvantaged students. *Education Code 32.103*



RETURN OF
EQUIPMENT

Except as provided below, a student who receives data processing equipment from the District under this policy shall return the equipment to the District not later than the earliest of:

1. Five years after the date the student receives the equipment;
2. The date the student graduates;
3. The date the student transfers to another district; or
4. The date the student withdraws from school.

If, at the time the student is required to return the equipment, the District determines that the equipment has no marketable value, the student is not required to return the equipment.

Education Code 32.106

UNIFORM
ELECTRONIC
TRANSACTIONS ACT

The District may agree with other parties to conduct transactions by electronic means. Any such agreement or transaction must be done in accordance with the Uniform Electronic Transactions Act. *Business and Commerce Code 43.*



The Superintendent or designee shall implement, monitor, and evaluate electronic media resources for instructional and administrative purposes.

AVAILABILITY
OF ACCESS

Access to the District's electronic communications system, including the Internet, shall be made available to students and employees primarily for instructional and administrative purposes and in accordance with administrative regulations. Limited personal use of the system shall be permitted by employees if the use:

1. Imposes no tangible cost on the District;
2. Does not unduly burden the District's computer or network resources; and
3. Has no adverse effect on an employee's job performance.

Access to the District's electronic communications system is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the system and shall agree in writing to comply with such regulations and guidelines. Noncompliance with applicable regulations may result in suspension or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violations of law may result in criminal prosecution as well as disciplinary action by the District.

ACCEPTABLE
USE

The Superintendent or designee shall develop and implement administrative regulations, guidelines, and user agreements, consistent with the purposes and mission of the District and with law and policy governing copyright. [See EFE]

INTERNET
SAFETY

The Superintendent or designee shall develop and implement an Internet safety plan that, to the greatest extent possible:

1. Controls students' access to inappropriate materials. as well



as to materials that are harmful to minors;

2. Ensures student safety and security when using electronic communications;
3. Prevents unauthorized access, including hacking and other unlawful activities; and
4. Restricts unauthorized disclosure, use, and dissemination of personally identifiable information regarding students.

FILTERING

Each District computer with Internet access shall have a filtering device service or 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 and as determined by the Superintendent or designee.

The Superintendent or designee shall enforce the use of such filtering devices. Upon approval from the Superintendent or designee, an administrator, supervisor, or other authorized person may disable the filtering device for bona fide research or other lawful purpose.

MONITORED USE

Electronic mail transmissions and other use of the electronic communications system by students and employees shall not be considered confidential. Any inappropriate use may warrant monitoring at any time by District staff, approved by the Superintendent or designee, to ensure appropriate use for educational or administrative purposes.

INTELLECTUAL PROPERTY RIGHTS

Students shall retain all rights to work they create using the District's electronic communications system.

As agents of the District, employees shall have limited rights to work they create using the District's electronic communications system. The District shall retain the right to use any product created in the scope of a person's employment even when the author is no longer an employee of the District.

DISCLAIMER OF LIABILITY

The District shall not be liable for users' inappropriate use of electronic communication resources or violations of copyright restrictions, users' mistakes or negligence, or costs incurred by users. The District shall not be responsible for ensuring the accuracy, age appropriateness, or usability of any information found on electronic resources, including the Internet.



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

The District will provide training 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 and safe use of this resource.

CONSENT
REQUIREMENTS

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 copyright owner or individual the owner specifically authorizes 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, if the student is a minor) or employee who created the work. [See CQ(EXHIBIT)]

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. [See CQ(EXHIBIT) and policies at FL]

FILTERING

The Superintendent will appoint a committee, to be chaired by the associate superintendent for technology, to select, implement, and maintain appropriate technology for filtering Internet sites containing material considered inappropriate or harmful to minors. All Internet access will be filtered for minors and adults on computers with Internet access provided by the school. The categories of material considered inappropriate and to which access will be blocked will include, but not be limited to: nudity/pornography; images or descriptions of sexual acts;



promotion of violence, illegal use of weapons, drug use, discrimination, or participation in hate groups; instructions for performing criminal acts (e.g., bomb making); and on-line gambling.

REQUESTS TO
DISABLE FILTER

The Superintendent or designee will consider requests from users who wish to use a blocked site for bona fide research or other lawful purposes.

SYSTEM ACCESS

Access to the District's electronic communications system 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/or supervision. Students will not be assigned individual e-mail accounts.
2. With the approval of the immediate supervisor and completion of required District network training, District employees will be granted access to the District's system. A teacher may apply for a class or project e-mail account and in doing so will be ultimately responsible for use of the account.
3. All District employees and students with accounts will be required to maintain password confidentiality by not sharing the password with others.
4. Any system user identified as a security risk or having violated District Acceptable Use Guidelines may be denied access to the District's system. Other consequences may also be assigned.
5. All users are required to review the Acceptable Use Guidelines annually for issuance or renewal of an account.

ASSOCIATE
SUPERINTENDENT
FOR
TECHNOLOGY
RESPONSIBILITIES

The assistant superintendent for technology 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 users of the District's system review annually the District policies and administrative regulations (Acceptable Use Guidelines) regarding such use.
3. Ensure that employees supervising students who use the District's system 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 student and employee safety on-line and proper use of the system.
6. Be authorized to disable a filtering device on the system for bona fide research or another lawful purpose, with approval from the Superintendent.
7. Set limits for data storage within the District's system, as needed.

**CAMPUS-LEVEL
COORDINATOR
RESPONSIBILITIES**

As the campus level coordinator for the network systems, the principal or designee will:

1. Be responsible for disseminating 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.

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 Superintendent or designee.

**INDIVIDUAL USER
RESPONSIBILITIES**

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

**ON-LINE
CONDUCT**

ALL USERS

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. Supervision and permission: student use of the computers and computer network is only allowed when supervised or when permission is granted by a staff member.
4. Attempting to log on or logging on to a computer or e-mail system by using another's password is prohibited; assisting others in violating this rule by sharing information or passwords is unacceptable.
5. Improper use of any computer or the network is prohibited. This includes the following:
 - a. Submitting, publishing, or displaying any defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented, or threatening materials or messages, whether public or private.
 - b. Using the network for financial gain or for political or commercial activity.
 - c. Attempting to harm or harming equipment, materials, or data.
 - d. Attempting to send or sending anonymous messages of any kind.
 - e. Using the network to access inappropriate material.
 - f. Knowingly placing a computer virus on a computer or the network.
 - g. Using the network to provide addresses or other personal information that others may use inappropriately.
6. Users shall not access information resources, files, and documents of another user without authorization.
7. System users may not disable, or attempt to disable, a filtering device on the District's electronic communications system.
8. Communications may not be encrypted so as to avoid



security review by system administrators.

9. System users may not use another person's system account without written permission from the campus administrator or District coordinator, as appropriate.
10. System users must purge electronic mail and data files in accordance with established retention guidelines.
11. 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.
12. System users should avoid actions that are likely to increase the risk of introducing viruses to the system, such as opening e-mail messages from unknown senders and loading data from unprotected computers.
13. 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.
14. System users may not waste District resources related to the electronic communications system.
15. System users may not gain unauthorized access to resources or information.

STUDENT USERS

Student users must adhere to the standards applicable to all users, listed above, as well as the two that follow:

1. Students may not distribute personal information about themselves or others by means of the electronic communications system; this includes, but is not limited to, personal addresses and telephone numbers.
2. Students should never make appointments to meet people whom they met on-line and should report to a teacher or administrator if they receive any request for such a meeting.



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 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 will result in the cancellation of system use privileges and will require restitution for costs associated with system restoration, hardware or software costs, as well as other appropriate consequences. [See DH, FN series, FO series, and the Student Code of Conduct]

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, despite the District's use of technology protection measures as required by law, use of the system may provide access to other electronic communications systems outside the District's 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 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. This could result in loss of credit for students or termination of employment for employees. [See DH]

PARTICIPATION IN CHAT ROOMS AND Students are prohibited from participating in any chat room or newsgroup accessed on the Internet. Such participation is permissible for employees. in accordance with District policies



NEWSGROUPS	and practices.
DISTRICT WEB SITE	<p>The District will maintain a District Web site for the purpose of informing employees, students, parents, and members of the community of District programs, policies, and practices. Requests for publication of information on the District Web site must be directed to the designated contact person. The assistant superintendent for technology, or designee, will establish guidelines for the development and format of Web pages controlled by the District.</p> <p>No personally identifiable information regarding a student will be published on a Web site controlled by the District without written permission from the student's parent.</p>
SCHOOL OR CLASS WEB PAGES	<p>Schools or classes may publish and link to the District's site Web pages that present information about the school or class activities, subject to approval from the campus principal. The campus principal will designate the staff member responsible for managing the campus's Web page [see CQ(EXHIBIT)]. Teachers will be responsible for compliance with District rules in maintaining their class Web pages. Any links from a school or class Web page to sites outside the District's computer system must receive approval from the campus principal or designee [see CQ(EXHIBIT)].</p>
NETWORK ETIQUETTE	<p>System users are expected to observe the following network etiquette:</p> <ol style="list-style-type: none"> 1. Use appropriate language: swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited. 2. Pretending to be someone else when sending/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.

**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 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.

**CONSEQUENCES
OF IMPROPER USE** Improper or unethical use may result in disciplinary actions consistent with the existing Student Code of Conduct 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 express 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 system 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 electronic communications system.

**TRANSFER OF
EQUIPMENT TO
STUDENTS** The following regulations will apply to all schools and departments regarding transfer of equipment to students under policy CQ:

1. Proposed projects to distribute equipment to students shall be sent to the associate Superintendent for technology for initial approval.



2. A student is eligible to receive data processing equipment under this regulation only if the student does not otherwise have home access to data processing equipment as determined by the school.
3. In transferring data processing equipment to students, a school shall give preference to educationally disadvantaged students as determined by the school.
4. Before transferring data processing equipment to a student, each school must have clearly identified:
 - a. A process to determine eligibility of students under policy CQ.
 - b. An application process that identifies the responsibility of the student regarding home placement, use, and ownership of the equipment.
 - c. A process to distribute and initially train students in the setup and care of the equipment.
 - d. A process to provide ongoing technical assistance for students using the equipment.
 - e. A process to determine ongoing student use of the equipment.
 - f. A process to determine any impact on student achievement the use of this equipment may provide.
 - g. A process for retrieval of equipment from students as necessary.



ELECTRONIC COMMUNICATION AND DATA
MANAGEMENT

CQ
(EXHIBIT)

The following exhibits are used by the District:

- Exhibit A: Electronic Mail and Additional Guidelines - 3 pages
- Exhibit B: School Web Page Guidelines - 5 pages
- Exhibit C: Principal Designee for School Web Page Approval - 1 page
- Exhibit D: Release Form for Publications, Video, and Electronic Display of Student Work - 2 pages
- Exhibit E: Release Form for Student Records - 1 page



EXHIBIT A

ELECTRONIC MAIL AND ADDITIONAL GUIDELINES

- Electronic Mail (e-mail) via the GroupWise Network Application
- User Security Responsibilities
- Maintenance of Local Hard Drives
- Software and Hardware Procurement

Electronic Mail

E-mail is one of the most used communications tools in both offices and classrooms.

The following points are important to keep in mind.

- The software and hardware that provides us e-mail capabilities has been publicly funded. For that reason, it should not be considered a private, personal form of communication. Although we do not have staff who actively monitor e-mail communications, the contents of any communication of this type would be governed by the Public Information Act. We would have to abide and cooperate with any legal request for access to e-mail contents by the proper authorities.
- Since e-mail access is provided as a normal operating tool for any employee who requires it to perform their job, individual staff e-mail addresses must be shared with interested parents and community members who request to communicate with staff in this fashion. We have no plans to produce and publish a District-wide list of e-mail addresses, but each campus and department should post a list of e-mail addresses for their staff through their Internet pages. Please contact your cluster technology coordinator for assistance in creating Internet pages that allow connections to staff via e-mail.
- Staff should be expected to return e-mail communications to parents or other public members who have a legitimate business request within 24 hours whenever possible. Requests from outside agencies for information do not fit into this same category and can be handled with a different timeline or in a manner consistent with previous experience in working with similar requests. Staff should not participate in e-mail surveys without District authorization.
- Incoming e-mail that is misaddressed will remain "undeliverable". We do not have the staff available to personally inspect all messages of this type and forward them to the proper person. Please be certain that you give out your correct e-mail address. All Internet pages containing lists of staff addresses should also contain a disclaimer that makes everyone aware that if e-mail is not responded to in a 24-hour timeframe, it may have been misaddressed and should be resent.
- Requests for personal information on students or staff members should not be honored via e-mail [see CQ(EXHIBIT E)]. It is critical for a personal contact to be made with any individual requesting personal information. This relates particularly to any requests for student



grades, discipline, attendance, or related information. In addition, security information such as username or password should not be sent via e-mail for any reason.

- During student contact time in the classroom, your e-mail notifier should be turned off to prevent interruptions. Staff members should set aside time at least once a day to check and respond to e-mail messages. E-mail does not have to be answered immediately; simply allow enough time so that the 24-hour turnaround time can be met in most instances.
- Since e-mail access is provided for school business related use, please do not forward messages that have no educational or professional value. An example would be any number of messages that show a cute text pattern or follow a "chain letter" concept. These messages should be deleted and the sender notified that messages of that nature are not appropriate to receive on your District e-mail account.
- Please use the "groups" function of our e-mail system appropriately. Do not send messages to an entire staff when only a small group of people actually needs to receive the message.
- Attachments to e-mail messages should include only data files. At no time should program files (typically labeled ".exe") be attached due to software licensing requirements. In addition, there exists the real possibility that any program files received as attachments over the Internet may include viruses or other very destructive capabilities once they are "launched" or started. If you receive an attachment like this, please delete the e-mail message immediately without saving or looking at the attachment.
- Subscriptions to Internet listservs should be limited to professional digests due to the amount of e-mail traffic generated by general subscriptions. Please use your personal Internet account to receive listserv subscriptions of a general nature, if one is available.
- Students will not be issued individual e-mail accounts. For any projects that involve e-mail communications, use either your District account as a facilitator to the activity, or, work with your cluster technology coordinator to activate a special project account for a limited time.
- Please notify your cluster technology coordinator or your campus technology assistant if you receive unsolicited e-mail, particularly if it is of a "hate mail" nature. We will attempt to track down the source of that e-mail and prevent you from receiving any additional unsolicited mail.

User Security Responsibilities

- Your username and password should be protected from unauthorized use at all times. Do not post any of this information where it can be viewed by others.
- Do not share your password via e-mail at any time. If a technology representative needs that information, they must request it in person.
- You should use your screen saver to secure your computer whenever it is not in use, and it should be password protected. (Refer to a network training manual for steps to do this.) Please activate the screen saver



manually (by clicking on the small red/yellows "x" icon in the lower right-hand corner of your desktop) whenever you leave the computer, to protect against unauthorized use. If you are "logged in" to the network, leaving a computer with the screen saver not password protected enables anyone to potentially access your gradebook, e-mail, and personal files.

Maintenance of Local Hard Drives

- On occasion, we need to reformat hard drives. Reformatting completely erases all contents of the hard drive. All district software such as Microsoft Office and Grade2, which is consistent throughout the District, will be reinstalled. All other approved software, purchased by the building, will need to be reinstalled by the Campus Technology Assistant. We will not reinstall unapproved copies of software nor will we be able to retrieve any personal data files. With this in mind, please keep any installation disks of specific school-purchased software (from those items pre-approved in the technology catalog) in an identified location at your campus should the need for reinstallation arise. Please be personally responsible for making backups of any data files that you store on your local hard drive.
- All computer and video hardware should be shut down each evening. This includes CPUs, monitors and VCRs. The exception to this would be laser printers. They can be left on since they include automatic power-saving features.

Software and Hardware Purchases

- The identified process for purchasing software is included in the technology catalog and can be found on the Internet at (<http://k-12.pisd.edu/techcat/techcat.htm>). No software packages can be purchased at the campus or department level without following that process.
- It is important to keep in mind that no software should, or will, be installed without documentation that shows the software purchase has gone through the process referenced above and that proper licensing has been purchased.
- Similarly, all hardware purchases should be for those items listed in the technology catalog since we have maintenance agreements on those items. For items not listed in the technology catalog, please work with your cluster technology coordinator for appropriate purchases.



EXHIBIT B

SCHOOL WEB PAGE GUIDELINES

Protocol/Responsibility

- Each school is responsible for the development and updates of their pages. The Instructional Technology department will offer training and support for designated staff members.
- It is strongly encouraged that the principal designates a Web page committee. This committee may be made up of administrators, teachers, paraprofessionals, parents, community members, and students. The chairman must be a designated staff member.*
- Each school is responsible for acquiring the PISD Publications, Video, Internet Consent and Release Agreement prior to posting any student's name, picture, art, written work, voice, verbal statements or portraits (video or still) on the school's web pages. This form must be signed by the parents and filed at the campus. This form is available at <http://12.pisd.edu/techs/release.htm>.
- Upon written approval (e-mail acceptable) by building principal or the designated staff member*, the Web page files will be posted to the District Web server by the Instructional Technology department. At no time will files be posted that are submitted directly by students.

*Designated staff member-someone employed by the school District, such as an administrator, a teacher, or paraprofessional. The designated staff member must be identified and approved in writing (using the form provided by Instructional Technology) by the building principal. This form is available at <http://k-12.pisd.edu/guide/schools/webpages/designee.htm>. This form is to be printed, completed, and sent to the instructional technology coordinator for your cluster.

Requirements

- Pages that contain time-sensitive information, such as calendars, school events, and staff information, must be updated monthly in ensure current, accurate information.
- The Instructional Technology Department will post Web page files as received.
- Web pages must be checked monthly to make sure that all links work correctly.
- All Web pages must have a title (which appears on the Web browser's title bar).
- Each school's main homepage must include the school's name, address, phone number, a link to Plano ISD, and a school contact's PISD e-mail address.
- Each page must (at minimum) contain a link back to the previous level in the school's site, and a link to the site's main navigational page.



- The Plano Independent School District Web servers are for educational use only. Contents of the site should give information and promote school activities (PTA, classes, staff, departments, sports, school projects, calendars, volunteering opportunities, etc.) Information concerning non-curricular student groups may not be posted to the school's Web pages. (Example: Chess Club, FCA, etc.)
- External Links (Links to sites and content that is not hosted on an official Plano ISD Web server)
 - Commercial Links

Certain fundraising information and links may be allowed, such as "shopfor-school.com" or "marketday.com". These company links should have approval District-wide. All other commercials, commercial transactions, or advertisements are prohibited on school pages.
 - Education Links

Elementary: External links should be discouraged on elementary school pages. This is largely due to the fact that the Curriculum and Instructional Technology departments actively research and provide sites that support and enrich curriculum through the District's instructional Web resources.
 - Secondary: External links should be allowed as approved by the building principal.

Note: In all cases where an "external link" (link to a site or content that is not hosted on an official Plano ISD Web server), is used on a school's Web site, the following disclaimer statement must be present on the school's main navigation page: Plano ISD is not responsible for contents on external sites or servers.

- All official school and District sites must be hosted on Plano ISD Web servers.
- Teachers may post personal classroom pages with their school's Web site following the same protocol and guidelines presented in this document.
- Files hosted on the Plano ISD Web server(s) and hyperlinks from these files should 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.
- Staff members' PISD e-mail addresses are posted, as public information, on the District's main Web site at <http://www.pisd.edu>. Staff members' PISD e-mail address should also be posted on each school's Web site. (It is recommended that schools also include telephone extensions and staff photos, if available.)
- The following student information is generally acceptable to include, if parent(s) have given permission/consent to use it per District release form, on a school's Web page.



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

No other personal information about a student is allowed, such as e-mail address, phone number, or home address.

- Unauthorized use of copyrighted material is prohibited. Giving credit (Web address or active link) to a company that has created a graphic, design, etc., for a school page may be allowed, unless the District filtering system blocks the site.
- If a school wants a Web page counter on its site, it must be an "invisible" counter type only.
- Prohibited items include:
 - Personal information about staff and parent volunteers: non-District e-mail addresses, non-District mailing address, and non-District phone numbers except as approved by the building principal. Example: PTSO/PTA/Booster Organization officer/contact requests to have their personal e-mail address listed in the appropriate area on the school's page(s) and principal approves the request. Note: Pictures and names of staff and parent volunteers will be allowed with principal's approval.
 - Student personal contact information of any kind.
 - Links to staff, volunteer, or student personal home pages.
 - Links to "non-official" PISD related sites that are hosted on remote/external (non-District) Web servers. Examples: athletic booster pages, PTA pages, teacher-created classroom pages, etc. However, booster organizations, PTA, teachers, etc., may post their pages on their school's Web site following the same protocol and guidelines presented in this document.
 - "Guest books," "chat areas," "message boards," or similar.
 - Links to sites that are not accessible inside the network (through the filtering system).

Web Publishing Recommendations

- The following information should be included on school pages: welcome from the principal, general information about the school (namesake, history, when the school opened, last renovation, etc.), event information (calendar, upcoming meetings, special programs, days off, early release days, etc.), SBIC information (names, addresses, and phone numbers of members, committee's role and mission, annual report, and action plan), information about the PTA or PTO (officers and board members with phone numbers so that newcomers can access them; events, programs, and volunteer opportunities), pertinent information from student and parent handbooks (policies and procedures on attendance, discipline, tardies, etc.), copy of school newsletter, link to attendance area information, link to test score information, recognition



of students and teachers, parenting information to help parents tutor or assist their children, and fundraising activities.

- Use a consistent style on the school's main pages. (Individual departments, grade levels, programs, etc., may vary, but the administrative and general information pages should maintain consistency in look and navigation.)
- Elementary schools should place a link to the District's Elementary Curriculum home page. The link can be placed on any of the school's pages as desired, but should be present on all "grade level" or "classroom" type pages. The address to use is
- <http://k-12.pisd.edu/currinst/elemen/elemen.htm>.
- Pages should be sized so they will display properly in a variety of screen resolutions. Pages should be previewed and tested at least at "640 x 480," "800 x 600," and "1024 x 768."
- Regular text entries on Web pages should be limited to the fonts "Arial" and "Times New Roman" on the PC, or "Helvetica" and "Times" on the Macintosh. Any special fonts should be saved and used as graphics to ensure that they display properly.
- Avoid color schemes or backgrounds that make the information on the page hard to read.
- Colors should be "Web safe" as much as possible, so they will display properly in 216 colors.
- Avoid using white text or links (white is difficult).
- Graphics should be used judiciously. Photos and other graphics should generally not exceed a total 100k (file size) per page.
- Animated GIF files should be used very sparingly and need to be relatively small. The amount, size, and type of graphics used have the most direct affect on the "load time" of Web pages.
- Video and audio files may be used when they are appropriate and are compressed properly. They are generally large files that take long "load times" for the user, and many times require some users (non-District networked machines) to have special plug-ins or viewers/players, in order to view or hear the files.

Web Technologies Supported on District Server(s)

- The District Web server does not support "cgi" script.
- The District Web server does not support Microsoft FrontPage Extensions.
- All District-networked computers utilize Java capable browsers. Currently, the District supported browser is Internet Explorer 6.
- All District-networked computers have the following plug-ins loaded:
Windows MediaPlayer Plugin (in addition, Windows MediaPlayer V.7.01 is also loaded as an application)

HyperStudio Plugin-V.4



Macromedia Flash and Director (Shockwave)-V.6 (MX)

RealPlayer G2-V.8

QuickTime Player-V.5.0.2

Adobe Acrobat Reader-V.5.0.5



EXHIBIT C

PRINCIPAL DESIGNEE FOR SCHOOL WEB PAGE APPROVAL

Please print this form (also available on-line at <http://k-12.pisd.edu/guide/schools/webpages/designee.htm>) and send the completed form through school mail to the instructional technology coordinator for your cluster.

East Cluster-

Central Cluster-Candy Atwood

West Cluster-Harriet Bell

School: _____

Principal Signature: _____

Date: _____

The following is my designated staff member, for the 2001-02 school year, who has the authority and responsibility for reviewing and approving the content of our school Web pages as described in the Plano ISD School Web Page Guidelines. An on-line copy of these guidelines may be found at <http://k-12.pisd.edu/guide/schools/webpages>.

Name (please print): _____

Phone extension: _____

E-mail Address: _____



EXHIBIT D

RELEASE FORM FOR PUBLICATIONS, VIDEO, AND ELECTRONIC DISPLAY OF STUDENT WORK
2001-02 PLANO INDEPENDENT SCHOOL DISTRICT
PUBLICATIONS, VIDEO, INTERNET CONSENT AND RELEASE AGREEMENT

Students who attend school in the Plano Independent School District are occasionally asked to be a part of school and/or District publicity, publications and/or public relations activities. In order to guarantee student privacy and ensure your agreement for your student to participate, the District asks that you sign this form and return a form to the school for each of your students.

The form referenced below indicates approval for the student's name, picture, work, voice, verbal statements or portraits (video or still) to appear in school publicity or District publications, videos, or on the District's website. For example, pictures and articles about school activities may appear in local newspapers or District publications. These pictures and articles may or may not personally identify the student. The pictures and/or videos may be used by the District in subsequent years.

AGREEMENT

Student and Parent/Guardian release to Plano ISD the student's name, picture, work, voice, verbal statements, and portraits (video or still) and consent to their use by PISD.

Plano ISD agrees that the student's name, work, voice, verbal statements, portraits or picture (video or still) shall only be used for public relations, public information, school or District promotion, publicity, and instruction

Student and Parent/Guardian understand and agree that:

- No monetary consideration shall be paid;
- Consent and release have been given without coercion or duress;
- This agreement is binding upon heirs and/or future legal representatives;
- The photo, video, or student statements may be used in subsequent years.

If the Student and Parent/Guardian wish to rescind this agreement they may do so at any time with written notice.

Effective Date of Agreement: _____

Student's Name (please print): _____

Student's Signature: _____

Parent/Guardian Name (please print): _____

Parent/Guardian Signature: _____

Pursuant to Texas Education Code, Section 26.009(b)(2)

PISD has no control of media use of pictures/statements which are taken without permission.



EXHIBIT E

RELEASE OF STUDENT RECORDS

I, _____ (name), give my permission and request the release of student record information of my child _____ to be provided to me electronically (child's name) by the District. The specific information and/or records requested are:

I understand that the transmittal of this material may not be available by secure methods and may be capable of observation, interception, or monitoring by others. Further, I understand the District cannot guarantee that the records will be received only by the requestor at the e-mail address provided. I request that the student record information request above be sent to _____, my e-mail address.

Student's Parent or Guardian: _____

Home Address: _____

E-mail Address: _____

Date: _____

Home Number: _____

Parent/Guardian Signature: _____

The above release assumes that the student records will be sent via e-mail or fax rather than through direct access to the Internet.

