

2361 ACCEPTABLE USE OF COMPUTER NETWORK/COMPUTERS  
AND RESOURCES

Purpose

The Internet, a global electronic information infrastructure, is a system of networks used by educators, business, the government, the military, and organizations. The district Internet system has not been provided as a public access or personal Internet service. Use of the district Internet system is limited to those activities that support education, enrichment, and career development.

As a learning resource, the Internet is similar to books, magazines, videos, CD-ROMS, and other information sources. The Palmyra School System considers the use of Internet as an educational resource that will follow district guidelines for selection and use. Because the Internet is a fluid environment the information which will be available to students is constantly changing; therefore, it is impossible to predict with certainty what information students might locate. Just as the purpose, availability, and use of media materials does not indicate endorsement of their contents by school officials, neither does making electronic information available to students implies endorsement of that content. Electronic communication activities are limited to educationally related activities and will occur within secure environments.

Internet Safety/Protection

The school district is in compliance with the Children's Internet Protection Act and has installed technology protection measures for all computers in the school district, including computers in media centers/libraries, that block and/or filter visual depictions that are obscene as defined in Section 1460 of Title 18, United States Code; child pornography, as defined in Section 2256 of Title 18, United States Code; are harmful to minors including any pictures, images, graphic image file or other visual depiction that taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or depicts, describes, or represents in a patently offensive way, with respect to what is suitable for minors, sexual acts or conduct; or taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

The school district will certify on an annual basis, that the schools, including media centers/libraries, in the district are in compliance with the Children's Internet Protection Act and the school district enforces the requirements of this policy.

This Policy also establishes Internet safety policy and procedures in the district as required in the Neighborhood Children's Internet Protection Act. Policy 2361 addresses access by minors to inappropriate matter on the Internet and World Wide Web; the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; unauthorized access, including "hacking" and other unlawful activities by minors online; unauthorized disclosures, use, and dissemination of personal identification information regarding minors; and measures designed to restrict minors' access to materials harmful to minors.

Notwithstanding blocking and/or filtering the visual depictions prohibited in the Children's Internet Protection Act, the Board shall determine other Internet material that is inappropriate for minors. The Board will provide reasonable public notice and will hold one annual public hearing during a regular monthly board meeting or during a designated special board meeting to address and receive public community input on the Internet safety policy - Policy and Regulation 2361.

#### Goals

The Board's goal in providing these services to students and staff is to promote educational excellence within the schools by facilitating resource sharing, innovation, and communication.

1. Teaching Environment: The network shall enhance the teaching environment for all teachers in the Palmyra Public Schools by expanding the personal contacts and information resources available to these teachers.
2. Curriculum Development: The network shall be available to serve the development of curricular activities of the Palmyra Public Schools in all subject areas and at all grade levels.

## Use

Palmyra students and staff use the Internet to participate in distance learning activities, to ask questions of and consult with experts, to communicate with other students and individuals, and to locate material to meet their educational information needs. The use of the Internet is a privilege, not a right. Inappropriate use may result in a cancellation of privileges. Our educational staff has a professional responsibility to work together to help students develop the intellectual skills needed to discriminate among informational sources, to identify information appropriate to their age and developmental levels, and to evaluate and use information obtained electronically to help meet their educational goals.

Electronic information research skills are now fundamental to preparation for citizenship and future employment. The Board expects that the staff will provide guidance and instruction to students in the appropriate use of such resources. The school district network is monitored constantly by an Internet filtering system called I-Gear, which is used to block objectionable Internet content.

In accordance with Bill A592, the district web site will not disclose any personally identifiable information about a student without receiving prior written consent from the student's parent or legal guardian on a form developed by the Department of Education. As used in this act, "personally identifiable information" means student names, student photos, student addresses, student e-mail addresses, student phone numbers, and locations and times of class trips.

## Expected Behavior

Students and staff are expected to demonstrate responsible behavior on the district computer network and all related hardware and software, just as they are in any instructional or non-instructional setting within the district.

Passwords and account information are not to be shared among staff or students.

The use of the Internet is a privilege. Students and staff are expected to abide by the generally accepted rules of network etiquette. These include (but are not limited to) the following:

1. Be polite. Do not get abusive in your messages to others. Use appropriate language. Do not swear; use vulgarities or other inappropriate language. Illegal activities are strictly forbidden.
2. Do not reveal your personal address or phone numbers of students or colleagues. Note that electronic mail (e-mail) is not guaranteed to be private. People who operate the system do have access to all mail. Messages relating to or support of illegal activities may be reported to the authorities. Do not use the network in such a way that you would disrupt the use of the network by other users. All communications and information accessible via the network should be assumed to be private property. You may not attempt to use or alter anyone else's network account. You may not break in or attempt to break into other computer systems. You may not create or share computer viruses. The system is protected by Norton Antivirus 7.5. You may not destroy another person's data. Transmission or reception of any material in violation of an U.S. or State regulation is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material, or material protected by trade secret. The network is protected by an Internet filtering system called I-Gear and a Cisco PIX Firewall that prevents unauthorized access to the district network.

#### Consequences

Consequences for misuse/abuse of the Internet (depending on the severity of the situation, the disciplinary process may include combinations of the following consequences):

1. Warning;
2. Loss of credit for the assignment;
3. Loss of credit for the unit;

4. Loss of privilege to use the Internet;
5. Loss of computer privileges in the Palmyra School District;
6. Referral to administration for discipline; and
7. Referral to authorities for processing.

After district staff have received in-service training and instruction in the use of the Internet System hardware and software they will be responsible for following the established usage policy.

The Palmyra School District maintains certain policies with regard to the use and security of its system. The Board reserves the right to log use of telecommunications and network use and to monitor file server space utilization by users. Network storage areas will be treated like school lockers as described in the district's search and seizure policy. They remain the sole property of the district and are subject to administrative search, by school officials, at any time, in the interests of school safety, discipline, enforcement of school rules and regulations and enforcement of the law. Any search of the aforesaid items by law enforcement officials shall only be conducted upon presentation of a proper search warrant. All users of our facilities are expected to be familiar with these policies.

Violations of this policy can lead to the suspension of a computer account pending investigation of circumstances. Serious violations of this policy will be referred directly to the appropriate academic or outside authorities. Unauthorized use of district computing facilities can be a criminal offense. The penalties may be as severe as suspension or dismissal from the district and/or criminal prosecution.

#### Terms and Conditions

1. Students must be monitored at all times by instructional staff.
2. Unauthorized attempts to gain privileged access or access to any account not belonging to you on any district system is not permitted.

3. Individual accounts cannot be transferred to or used by another individual. Sharing passwords is not permitted.
4. Each user is responsible for all matters pertaining to the proper use of their account; this includes choosing safe passwords.
5. It is the student's responsibility to become familiar with the rules and procedures regarding the district policies involving use of the district network.
6. No district system may be used as a vehicle to gain unauthorized access to other systems.
7. No district system may be used for commercial or for profit activities. Use for product advertisement or political lobbying is also prohibited.
8. No district system may be used for unethical, illegal criminal purposes.
9. Any user who finds a possible security lapse on any district system is obliged to report it to an administrator. Don't attempt to use the system under these conditions until the administrator has investigated the problem.
10. Please keep in mind that many people use the district systems for daily work. Job related activities always take precedence over any personal activities.
11. Electronic mail on all district systems is as private as we can make it. Attempts to read another person's electronic mail or other protected files will be treated with the utmost seriousness. The system administrators will not read mail or non-word-readable files unless deemed necessary in the course of their duties, and will treat the contents of those files as private information at all times.
12. Use of the district system for commercial uses, except by approved outside organizations, is strictly prohibited. Such prohibited uses include, but are not limited to, development of programs, data processing or computations for commercial use and preparation and presentation of advertising material.

13. Students are not permitted to use electronic mail and other forms of direct electronic communication unless engaged in an instructional activity sanctioned and monitored by an instructional staff member. Chat rooms are not permitted.
14. The school district does not condone or tolerate the unauthorized copying or use of licensed computer software. You must adhere to the district's contractual responsibilities and comply with all copyright laws. Anyone who violates this policy may be subject to immediate suspension of system access pending investigation by the Principal/Technology Supervisor. An individual engaged in the unauthorized copying or use software may also face civil suit, criminal charges, and/or penalties and fines. Subject to the facts and circumstances of each case, such individuals shall be solely responsible for their defense and any resulting liability.
15. No district system may be used for sending nuisance messages, such as chain letters and obscene or harassing messages.
16. The Children's Internet Protection Act does not permit an administrator or supervisor or "person authorized" to disable the technology protection measure to enable access for bona fide research or other lawful purpose.
17. Every staff member will be oriented regarding these policies and procedures at the beginning of every school year.
18. All network activities are subject to the aforementioned rules and regulations.
19. All the above pertain to both students and all school district personnel.

The district may modify these rules at any time by publishing the modified rules(s) on the system.

N.J.S.A. 2A:38A-3  
Federal Communications Commission: Children's Internet  
Protection Act.

Adopted: 16 January 2007

R 2361 ACCEPTABLE USE OF COMPUTER NETWORK/COMPUTERS  
AND RESOURCES

The school district provides computer equipment, computer services, and Internet access to its pupils and staff for educational purposes only. The purpose of providing technology resources is to improve learning and teaching through research, teacher training, collaboration, dissemination and the use of global communication resources. The "system administrators" referred to herein as employees of the school district who administer the school district computer network/computers and the system administrators reserve the right to monitor all activity on network/computer facilities/computers.

Because of the complex association between so many government agencies and computer networks/computers, the end user of these computer networks/computers must adhere to strict regulations. Regulations are provided here so that staff, community, and pupil users and the parent(s) or legal guardian(s) of pupils are aware of their responsibilities. The school district may modify these regulations at any time by publishing modified regulations on the network and elsewhere. The signatures of the pupil and his/her parent(s) or legal guardian(s) on the district-approved consent and waiver agreement are legally binding and indicate that the parties have read the terms and conditions carefully, understand their significance, and agree to abide by the rules established under Policy and Regulation No. 2361.

Pupils are responsible for good behavior on computer networks/computers just as they are in a classroom or a school hallway. Communications on the computer network/computers are often public in nature. Policies and Regulations governing behavior and communications apply. The school district's networks, Internet access and computers are provided for pupils to conduct research and communicate with others. Access to computer network services/computers is given to pupils who agree to act in a considerate and responsible manner. Parent permission is required. Access is a privilege—not a right. Access entails responsibility. Individual users of the district computer network/computers are responsible for their behavior and communications over the computer network/computers. It is presumed that users will comply with district standards and will honor the agreements they have signed.

Beyond the clarification of such standards, the district is not responsible for the actions of individuals utilizing the computer network/computers who violate the policies and regulations of the Board.

Computer network/computer storage areas shall be treated in the same manner as other school storage facilities. Computer network/computer administrators may review files and communications to maintain system integrity and ensure that users are using the system responsibly. Users should not expect that files stored on district servers will always be private.

Within reason, freedom of speech and access to information will be honored. During school, teachers of younger pupils will guide them toward appropriate materials. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, movies, radio and other potentially offensive media. As outlined in Board policy and procedures on pupil rights and responsibilities, copies of these are available in school offices. Behavior including but not limited to the following are prohibited:

1. Sending or displaying offensive messages or pictures;
2. Using obscene language and/or accessing visual depictions that are obscene as defined in section 1460 of Title 18, United States Code;
3. Using or accessing visual depictions that are child pornography, as defined in section 2256 of Title 18, United States Code;
4. Using or accessing visual depictions that are harmful to minors including any pictures, images, graphic image file or other visual depiction that taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or
5. Depicts, describes, or represents in a patently offensive way, with respect to what is suitable for minors, sexual acts or conduct; or taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

6. Harassing, insulting or attacking others;
7. Damaging computers, computer systems or computer network/computers;
8. Violating copyright laws;
9. Using another's password;
10. Trespassing in another's folders, work or files;
11. Intentionally wasting limited resources;
12. Employing the computer network/computers for commercial purposes; and/or
13. Engaging in other activities that do not advance the educational purposes for which computer network/computers are provided.

#### INTERNET SAFETY

##### Compliance with Children's Internet Protection Act

The school district has technology protection measures for all computers in the school district, including computers in media centers/libraries, that block and/or filter visual depictions that are obscene, child pornography and harmful to minors as defined in 2, 3, and 4 above and in the Children's Internet Protection Act. The school district will certify the schools in the district, including media centers/libraries are in compliance with the Children's Internet Protection Act and the district enforces Policy 2361.

##### Compliance with Neighborhood Children's Internet Protection Act

Policy 2361 and this Regulation establishes an Internet safety policy and procedures to address:

1. Access by minors to inappropriate matter on the Internet and 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 online;
4. Unauthorized disclosures, use, and dissemination of personal identification information regarding minors; and
5. Measures designed to restrict minors' access to materials harmful to minors.

Notwithstanding the visual depictions defined in the Children's Internet Protection Act and as defined in 2, 3, and 4 above, the Board shall determine Internet material that is inappropriate for minors. The Board will provide reasonable public notice and will hold one annual public hearing during a regular monthly Board meeting or during a designated special Board meeting to address and receive public community input on the Internet safety policy - Policy and Regulation 2361.

#### Information Content and Uses of the System

Users agree not to publish on or over the system any information which violates or infringes upon the rights of any other person or any information which would be abusive, profane or sexually offensive to an average person, or which, without the approval of the system administrators, contains any advertising or any solicitation of other members to use goods or services. The user agrees not to use the facilities and capabilities of the system to conduct any business or solicit the performance of any activity, which is prohibited by law.

Because the school district provides, through connection to the Internet, access to other computer systems around the world, pupils and their parent(s) or legal guardian(s) understand that the Board and system administrators have no control over content. While most of the content available on the Internet is innocuous and much of it a valuable educational resource, some objectionable material exists. The Board will provide pupil access to Internet resources only in supervised environments and has taken steps to lock out objectionable areas to the extent possible, but potential dangers remain. Pupils and their parent(s) or legal guardian(s) are advised that some systems may contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or otherwise illegal material. The Board and the system administrators do not

condone the use of such materials and do not permit usage of such materials in the school environment. Parent(s) or legal guardian(s) having accounts on the system should be aware of the existence of such materials and monitor home usage of the school district computer network. Pupils knowingly bringing such materials into the school environment will be disciplined in accordance with Board policies and regulations and such activities may result in termination of such pupils' accounts on the computer network and their independent use of computers.

#### On-line Conduct

Any action by a pupil or other user of the school district's computer network/computers that is determined by a system administrator to constitute an inappropriate use of computer network/computers resources or to improperly restrict or inhibit other members from using and enjoying those resources is strictly prohibited and may result in limitation on or termination of an offending member's account and other action in compliance with the Board policy and regulation. The user specifically agrees not to submit, publish, or display any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or otherwise illegal material; nor shall a user encourage the use, sale, or distribution of controlled substances. Transmission of material, information or software in violation of any local, state or federal law is also prohibited and is a breach of the Consent and Waiver Agreement.

Users and their parent(s) or legal guardian(s) specifically agree to indemnify the Palmyra School District and the system administrators for any losses, costs, or damages, including reasonable attorneys' fees incurred by the Board relating to, or arising out of any breach of this section by the user.

Computer network/computer resources are to be used by the user for his/her educational use only; commercial uses are strictly prohibited.

#### Software Libraries on the Network

Software libraries on the network are provided to pupils as an educational resource. No pupil may install, upload, or download software without the expressed consent of the system administrator. Any software having the purpose of damaging other members' accounts on the school district computer network/computers (e.g., computer viruses) is specifically

prohibited. The system administrators, at their sole discretion, reserve the rights to refuse posting of files and to remove files. The system administrators, at their sole discretion, further reserve the right to immediately limit usage or terminate the account or take other action consistent with the Board's policies and regulations of a member who misuses the software libraries.

#### Copyrighted Material

Copyrighted material must not be placed on any system connected to the computer network/computers without the author's specific written permission. Only the owner(s) or persons they specifically authorize may upload copyrighted material to the system. Members may download copyrighted material for their own use in accordance with Policy and Regulation Nos. 2531, Copying Copyrighted Materials. Any member may also noncommercially redistribute a copyrighted program with the expressed written permission of the owner or authorized person. Permission must be specified in the document, on the system, or must be obtained directly from the author.

#### Public Posting Areas (Message Boards/Usenet Groups)

Usenet messages are posted from systems connected to the Internet around the world and the school district system administrators have no control of the content of messages posted from these other systems. To best utilize system resources, the system administrators will determine which Usenet groups are most applicable to the educational needs of the school district and will carry these groups on the school district computer network. The system administrators, at their sole discretion, may remove messages posted locally that are deemed to be unacceptable or in violation of the Board policies and regulations. The system administrators, at their sole discretion, further reserve the right to immediately terminate the account of a member who misuses the message boards or Usenet groups.

#### Real-time, Interactive, Communication Areas

The system administrators, at their sole discretion, reserve the right to monitor and immediately limit the use of the computer network/computers or terminate the account of a member who misuses real-time conference features (talk/chat/Internet relay chat).

### Electronic Mail

Electronic mail ("E-mail") is an electronic message sent by or to a member in correspondence with another person having Internet mail access. All messages sent and received on the school district computer network must have an educational purpose and are subject to review. Messages received by the system are retained on the system until deleted by the recipient or for a maximum of fifteen days. A canceled account will not retain its E-mail. Members are expected to remove old messages within fifteen days or the system administrators may remove such messages. The system administrators may inspect the contents of E-mail sent by one member to an addressee, or disclose such contents to other than the sender or a recipient when required to do so by the Board policy, regulation or other laws and regulations of the State and Federal governments. The Board reserves the right to cooperate fully with local, state, or federal officials in any investigation concerning or relating to any E-mail transmitted on the school district computer network/computers.

### Disk Usage

The system administrators reserve the right to set quotas for disk usage on the system. A member who exceeds his/her quota of disk space will be advised to delete files to return to compliance with predetermined quotas. A member who remains in noncompliance of disk space quotas after seven school days of notification will have their files removed by a system administrator.

### Security

Security on any computer system is a high priority, especially when the system involves many users. If a member feels that he/she can identify a security problem on the computer network, the member must notify a system administrator. The member should not inform individuals other than the system administrators or other designated members of the school district staff of a security problem. Professional staff may allow individuals who are not members to access the system through the staff personal account as long as the staff person does not disclose the password of the account to the individuals and understands that the staff person assumes responsibility for the actions of individuals using his/her account. Members may not

otherwise allow others to use their account and password. Passwords to the system should not be easily guessable by others, nor should they be words, which could be found in a dictionary. Attempts to log in to the system using either another member's account or as a system administrator will result in termination of the account. Members should immediately notify a system administrator if a password is lost or stolen, or if they have reason to believe that someone has obtained unauthorized access to their account. Any member identified as a security risk will have limitations placed on usage of the computer network/computers or may be terminated as a user and be subject to other disciplinary action.

#### Vandalism

Vandalism will result in cancellation of system privileges and other disciplinary measures in compliance with the District's discipline code. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the system, or any of the agencies or other computer network/computers that are connected to the Internet backbone or of doing intentional damage to hardware or software on the system. This includes, but is not limited to, the uploading or creation of computer viruses.

#### Printing

The printing facilities of the computer network/computers should be used judiciously. Printing for other than educational purposes is prohibited.

#### Internet Sites and the World Wide Web

The system administrator may establish an Internet site(s) on the World Wide Web or other Internet locations. Such sites shall be administered and supervised by the system administrator, who shall ensure that the content of the site complies with federal, state and local laws and regulations as well as Board policies and regulations.

#### Violations

Violations of the Acceptable Use of Computer Network/Computers and Resources may result in a loss of access as well as other disciplinary or legal action. Disciplinary action shall be taken as indicated in Policy and Regulation Nos. 2361, Acceptable Use of Computer Network/Computers and Resources, No. 5600, Pupil Discipline, No. 5610, Suspension and No. 5620, Expulsion as well as possible legal action and reports to the legal authorities and entities.

#### Determination of Consequences for Violations

The particular consequences for violations of this policy shall be determined by the Non-Supervisor/Coordinator of Technology in matters relating to the use of computer networks/computers and by the Principal in matters of school suspension. The Superintendent or designee and the Board shall determine when school expulsion and/or legal action or actions by the authorities are the appropriate course of action.

Individuals violating this policy shall be subject to the consequences as indicated in Regulation No. 2361 and other appropriate discipline, which includes but is not limited to:

1. Use of Computer Network/Computers only under direct supervision;
2. Suspension of network privileges;
3. Revocation of network privileges;
4. Suspension of computer privileges;
5. Revocation of computer privileges;
6. Suspension from school;
7. Expulsion from school; and/or
8. Legal action and prosecution by the authorities.

Decisions of the Non-Supervisor/Coordinator of Technology may be appealed in accordance with Policy No. 5710 Pupil Grievances.

2362 ELECTRONIC MAIL

School district personnel shall adhere to the following guidelines when sending or receiving messages via internal or external E-Mail:

1. All messages shall pertain to legitimate school business.
2. Personnel shall not reveal passwords to others. If a staff member believes that a password has been lost or stolen, or that E-mail has been accessed by someone without authorization, he/she should contact the Help Desk immediately. E-mail windows should not be left open on the screen when the computer is left unattended.
3. Messages and E-mail files shall be deleted in a timely manner. The network system operator will delete messages that are retained after ninety days unless other arrangements are approved by the technology supervisor.
4. To ensure that federal copyright laws are not violated, staff shall not send messages that contain text without the author's permission.
5. Staff shall not send messages:
  - a. That contain material that may be defined by a reasonable person as obscene; messages that are racist, sexist or promote illegal or unethical activity; or messages that violate the district's affirmative action policy;
  - b. That are personal in nature and not related to the business of the district;
  - c. That are broadcast to a large group of other personnel without supervisory permission;
  - d. That contain confidential information to persons not authorized to receive that information.

6. Personnel shall become familiar with the district's policies and regulation on staff and student access to networked information resources before initiating E-mail use.

Employees learning of any misuse of the E-mail systems shall notify the Technology Supervisor immediately.

The district's electronic E-mail systems exist to assist staff and faculty in carrying out the mission of the school district. These systems, including the equipment and the data stored on them, and all messages contained in the systems, are, and remain at all times, the property of the Board of Education.

The district E-mail system is provided at the expense of the Board of Education to permit employees to communicate with each other internally and with individuals, educational institutions, agencies and businesses outside the district. E-mail rights that may be extended to an employee include internal district E-mail and external district E-mail through the Internet. All communications via district E-mail shall be for school related purposes only.

The Board of Education retains the right to access, review, copy and delete any messages sent, received or stored on the E-mail system.

The use of the E-mail system to engage in any communications that violate Federal, State, local or district law, code, policy, or regulation is prohibited. This includes sending any messages that are defamatory, obscene, harassing, or that violate the district affirmative action policy. Staff members who do not comply shall lose E-mail privileges. Other disciplinary action as appropriate may also apply.

The Superintendent shall develop regulations to administer this policy and shall approve those personnel who are given internal and external district Internet E-mail access.

Adopted: 20 February 2007