Aledo ISD – Internet Safety Policy

INTRODUCTION

It is the policy of the Aledo Independent School District (AISD) to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act ("CIPA"). It is the goal of this policy not only to prevent and protect, but to educate employees, students, parents and the community of AISD in Internet safety. The CIPA guidelines for an Internet Safety Policy have also been incorporated by AISD into its Acceptable Use Agreement.

The Children's Internet Protection Act, enacted December 21, 2000, requires recipients of federal technology funds to comply with certain Internet filtering and policy requirements. Schools and libraries receiving funds for Internet access and/or internal connection services must also meet the Internet safety policies of the Neighborhood Children's Internet Protection Act that addresses the broader issues of electronic messaging, disclosure of personal information of minors, and unlawful online activities.

This policy is intended to be read together with AISD's Acceptable Use Policies for Technology and the Internet. All limitations and penalties set forth in the Acceptable Use Policies are deemed to be incorporated into this policy. Terms used in this policy which also appear in the Children's Internet Protection Act have the meanings defined in the Children's Internet Protection Act.

COMPLIANCE WITH THE REQUIREMENTS OF CIPA:

Technology Protection Measures

A Technology Protection Measure is a specific technology that blocks or filters Internet access. It must protect against access by adults and minors to visual depictions that are obscene, involve child pornography, or are harmful to minors. AISD utilizes a sophisticated content filtering system, on all computers that access the Internet, which is compliant with CIPA and NCIPA.

Access to Inappropriate Material

To the extent practical, Technology Protection Measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual and textual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to administrative approval, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Any attempt to bypass, defeat or circumvent the Technology Prevention Measures is punishable as a violation of this policy and of the Acceptable Use Policies.

Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the AISD online computer network when using electronic mail, chat rooms, blogging, instant messaging, online discussions and other forms of direct electronic communications. Without limiting the foregoing, access to such means of communication is strictly limited by the Acceptable Use Policies.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Supervision and Monitoring

It shall be the responsibility of all professional employees (pedagogical and administrative staff) of AISD to supervise and monitor usage of AISD's computers, computer network and access to the Internet in accordance with this policy, the Acceptable Use Policies, and the Children's Internet Protection Act. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Chief Technology Officer or designated representatives.

Education

AISD will advocate and educate employees, students, parents and the AISD community on Internet safety and "cyber-bullying." Education will be provided through such means as professional development training and materials to employees, PTO presentations, CyberSmart week, and the AISD website.

Cyber-bullying

The Acceptable Use Policies include provisions intended to prohibit and establish penalties for inappropriate and oppressive conduct, including cyber-bullying.

AISD is a place of tolerance and good manners. Students may not use the network or any School District computer facilities for hate mail, defamatory statements, statements intended to injure or humiliate others by disclosure of personal information (whether true or false), personal attacks on others, and statements expressing animus towards any person or group by reason of race, color, religion, national origin, gender, sexual orientation or disability.

Network users may not use vulgar, derogatory, or obscene language.

Network users may not post inappropriate anonymous messages or forge e-mail or other messages.

Furthermore, School District computers and network facilities may not be used for any activity, or to transmit any material, that violates United States, State of Texas or local laws. This includes, but is not limited to any threat or act of intimidation or harassment against another person.

Aledo ISD - Acceptable Use Procedures (AUP) - Students

Aledo ISD (AISD) expects that all students will use technology, telecommunications and/or Internet tools in appropriate ways for the performance of tasks associated with their learning and assignments. Toward that end, AISD staff will guide students in the proper, effective, and acceptable use of telecommunications, electronic mail (messaging), Internet, and other technology usage. These procedures apply to any use of technology within district property or at district sponsored events regardless of who owns the technology.

1. Communication over networks and/or Internet should not be considered private. Network and/or Internet supervision and maintenance may require review and inspection of directories or messages. Messages may sometimes be diverted accidentally to a destination other than the one intended. Privacy in these communications is not guaranteed. The district reserves the right to access stored records in cases where there is reasonable cause to expect wrongdoing or misuse of the system. Courts have ruled that old messages may be subpoenaed, and network supervisors may examine communications in order to ascertain compliance with network guidelines for acceptable use.
2. AISD will specify those behaviors which are permitted and those which are not permitted, as well as appropriate procedures to guide students use. In general, students are expected to communicate in a respectful manner consistent with state laws governing the behavior of school students and with federal laws governing copyrights. Electronic messaging and telecommunications and/or Internet are not to be utilized to share confidential information about other students.
3. AISD encourages students to make use of telecommunications and/or Internet to explore educational topics, conduct research, and contact others in the educational world. AISD anticipates that new systems will expedite the sharing of effective practices and lessons across the district; and will help students stay on the leading edge of learning by forming partnerships with others across the nation and around the world.

Student Access to Networked Information Resources and/or Internet Procedures

1. The network and/or Internet are provided for students to conduct research and communicate with others as directed and supervised by staff. Communications over the network and/or Internet are often public in nature, therefore general rules and standards for respectful behavior and communications will apply. Safety and security when using electronic messaging, chat rooms, and other forms of direct electronic communications is essential.
2. Electronic messaging, telecommunications and Internet are not to be utilized by students to share confidential information about themselves or other students because messages are not entirely secure. Unauthorized disclosure, use and dissemination of personal information regarding minors will not be permitted.
3. Network administrators may review files and communications to maintain system integrity and to ensure that students are using the system responsibly. Users should not expect that files stored on district servers or any other storage device will be private, (i.e. diskettes, CD ROM, hard drives, flash drives, back-ups, etc.).

The following behaviors are not permitted on district networks and/or the Internet:

1. Sharing confidential information regarding students
2. Sending or displaying offensive messages or pictures
3. Assisting a campaign for election of any person to any office or for the promotion or opposition to any ballot proposition
4. Using obscene language
5. Harassing, insulting, or attacking others
6. Engaging in practices that threaten the network (e.g. downloading files that may contain a virus)
7. Unauthorized access to any network and/or network devices (e.g. hacking)
8. Violating copyright laws
9. Using others' passwords
10. Trespassing in others' folders, documents or files
11. Intentionally wasting limited resources

12. Employing the network and/or Internet for commercial purposes
13. Violating regulations prescribed by the network provider
14. Promoting, supporting, or celebrating religion or religious institutions

The Technology department will report inappropriate behaviors to the student's teacher who will take appropriate disciplinary action. Access to e-mail and other telecommunications and/or Internet is a privilege and violations of these procedures may result in a loss of access and/or disciplinary action up to and including expulsion. When applicable, law enforcement agencies may be involved.

Each student will sign an acceptable use agreement before establishing an account or continuing their use beyond August 1, 2010.

Electronic Messaging, Internet Usage, and Other Technology Usage Procedures

In order to ensure compliance with local, state, and federal computer crime laws, copyright laws, and to prevent inappropriate and non-company related use of AISD Communication and Information Systems by AISD Students and to protect AISD from being victimized by malicious acts of compromising organization assets, the following are AISD's regulations on the use of AISD Communication and Information Systems and/or Internet:

1. AISD Communication and Information Systems and/or Internet are not to be used in a way that may be disruptive, illegal, offensive to others, or harmful to morale, including unauthorized access and other unlawful activities. AISD maintains a process for monitoring student usage of AISD's Communication and Information Systems and/or Internet and will fully investigate suspected abuse. Students are responsible for preventing misuse of their computer equipment and should take reasonable and appropriate precautions to protect AISD's systems, including securing their computers (logging off before leaving.) AISD Communication and Information Systems and/or Internet are not to be used as personal bulletin services. AISD Communication and Information Systems and/or Internet are not to be used to transmit or knowingly receive vulgar, profane, insulting, or offensive messages, including racial, sexual slurs or jokes, harassing or threatening messages or pornography. AISD is required to comply with all applicable federal laws and will report to authorities any individual accessing, transmitting, or knowingly receiving illegal information through an AISD Communications and Information System and/or Internet, including child pornography and illegally obtained software or other media.
2. Students using AISD Communication and Information Systems and/or Internet are to use such services in a respectful manner so as not to damage the reputation of the organization. AISD Communication and Information Systems and/or Internet are to be used in compliance with the Student Handbook. AISD may choose to hold a student liable for any damage to AISD's reputation or systems as a result of a student's misuse or AISD's Communication and Information Systems and/or Internet.
3. Files that are downloaded from the Internet must be scanned with up-to-date virus detection software before installation or executions. All appropriate precautions must be taken to detect for a virus and, if necessary, to prevent its spread. The introduction of viruses, or malicious tampering with any computer system, is expressly prohibited. Questions on how to scan with virus detection software should be directed to the Help Desk. All identified viruses must be reported to the Help Desk.
4. Unauthorized students shall not place company confidential or proprietary material (including but not limited to copyrighted software, internal correspondence, or e-mail) on any publicly accessible Internet computer. Sensitive material transferred over the Internet may be at risk of detection by a third party without precautions. Students must exercise caution and care when transferring such material in any form. AISD confidential information is not to be transmitted or forwarded to outside individuals or companies not authorized to receive the information or AISD students who do not have an approved educational need for the information.. Alternate Internet Service

Provider (ISP) connections to AISD's internal network are not permitted. Examples of ISP's are America Online, Microsoft Network, Internet America, etc.

5. Unless otherwise noted, all software on the Internet should be considered copyrighted work. Therefore, students are prohibited from downloading software and/or modifying any such files without consulting their teacher. Students are required to adhere to all licensing and copyright laws and cannot use electronic communications systems to send (upload) or receive (download) copyrighted materials including software.
6. AISD reserves the right to restrict access to any materials that are inappropriate to minors and/or illegal materials. AISD also reserves the right to restrict access to and/or filter any type of direct communications (including electronic messaging and chat rooms) that are outside of the AISD Communication and Information Systems and/or Internet.
7. Vandalism is prohibited. Any malicious attempt to harm or destroy AISD equipment or materials, data of another user of the AISD's system, or any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to compromise, degrade, or disrupt system performance may be viewed as violations of AISD policies and administrative regulations and, possibly, as criminal activity under applicable state and federal laws. This includes, but is not limited to, the uploading or creating of computer viruses.
8. AISD Communication and Information Systems and/or Internet are AISD property and are not private. Students do not have a personal privacy right in any material created, stored, received or sent in or through AISD Communication and Information Systems and/or Internet. By using AISD Communication and Information Systems and/or Internet, all students knowingly and voluntarily consent of their usage of these systems being monitored and acknowledge and agree to AISD's right to conduct such monitoring. AISD, in its sole discretion, reserves the right to access, monitor, copy, transcribe, forward, download, capture, and/or disclose all communications sent via any AISD Communication and Information System and/or Internet at any time, with or without prior notice. Violations of AISD's procedures on use of its Communications and Information Systems and/or Internet may result in disciplinary action up to and including expulsion.

Internet Safety Procedures

AISD currently utilizes DeepNines for monitoring and filtering Internet traffic. Each year we evaluate whether to upgrade or purchase new and other products to give the organization and the services we provide the protection needed. Internet filtering blocks or filters Internet access. It protects against access by adults and minors to visual depictions that are obscene, child pornography, or - with respect to use of computers with internet access by minors – harmful to minors. It may be disabled for adults engaged in bonafide research or other lawful purposes. It includes monitoring the online activities of minors.

AISD internet filtering prevents access by minors to inappropriate matter on the Internet and World Wide Web. It also monitors electronic messaging, chat rooms, and other forms of direct electronic communications and unauthorized accessing and other unlawful activities online. AISD is committed to the education of minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber-bullying awareness and response.

Aledo ISD - Acceptable Use Procedures (AUP) - Staff

Aledo ISD (AISD) expects that all employees with computers will learn to use electronic mail and telecommunications and/or Internet tools and apply them daily in appropriate ways to the performance of tasks associated with their positions and assignments. Toward that end, AISD will provide staff with training in the proper and effective use of telecommunications, electronic mail (email), Internet, and PC usage.

1. Communication over networks and/or Internet should not be considered private. Network and/or Internet supervision and maintenance may require review and inspection of directories or messages. Messages may sometimes be diverted accidentally to a destination other than the one intended. Privacy in these communications is not guaranteed. The district reserves the right to access stored records in cases where there is reasonable causes to expect wrongdoing or misuse of the system. Courts have ruled that old messages may be subpoenaed, and network supervisors may examine communications in order to ascertain compliance with network guidelines for acceptable use.
2. AISD will specify those behaviors which are permitted and those which are not permitted, as well as appropriate procedures to guide employee use. In general, employees are expected to communicate in a professional manner consistent with state laws governing the behavior of school employees and with federal laws governing copyrights. Electronic mail and telecommunications and/or Internet are not to be utilized to share confidential information about students or other employees.
3. AISD encourages staff to make use of telecommunications and/or Internet to explore educational topics, conduct research, and contact others in the educational world. AISD anticipates that the new systems will expedite the sharing of effective practices and lessons across the district; and will help staff stay on the leading edge of practice by forming partnerships with others across the nation and around the world.

Staff Access to Networked Information Resources and/or Internet Procedures

1. Staff will employ electronic mail on a daily basis at work as a primary tool for communications. The district may rely upon this medium to communicate information, and all staff will be responsible for checking and reading messages daily.
2. The network and/or Internet are provided for staff and students to conduct research and communicate with others. Communications over the network and/or Internet are often public in nature, therefore general rules and standards for professional behavior and communications will apply. Safety and security when using electronic mail, chat rooms, and other forms of direct electronic communications is essential.
3. Electronic mail, telecommunications and Internet are not to be utilized by employees to share confidential information about students or other employees because messages are not entirely secure. Unauthorized disclosure, use and dissemination of personal information regarding minors will not be permitted.
4. Network administrators may review files and communications to maintain system integrity and to ensure that staff members are using the system responsibly. Users should not expect that files stored on district servers or any other storage device will be private, (i.e. diskettes, CD ROM, hard drives, flash drives, or back-ups).

The following behaviors are not permitted on district networks and/or the Internet:

1. Sharing confidential information regarding students or employees
2. Sending or displaying offensive messages or pictures
3. Assisting a campaign for election of any person to any office or for the promotion or opposition to any ballot proposition
4. Using obscene language
5. Harassing, insulting, or attacking others
6. Engaging in practices that threaten the network (e.g. downloading files that may contain a virus)
7. Unauthorized access to any network and/or network devices (e.g. hacking)
8. Violating copyright laws
9. Using others' passwords

10. Trespassing in others' folders, documents or files
11. Intentionally wasting limited resources
12. Employing the network and/or Internet for commercial purposes
13. Violating regulations prescribed by the network provider
14. Promoting, supporting, or celebrating religion or religious institutions

The Technology department will report inappropriate behaviors to the employee's supervisor who will take appropriate disciplinary action. Access to e-mail and other telecommunications and/or Internet is a privilege and violations of these procedures may result in a loss of access and/or disciplinary action up to and including termination. When applicable, law enforcement agencies may be involved.

Each employee will sign an acceptable use agreement before establishing an account or continuing their use beyond August 1, 2010.

Email Usage, Internet Usage, and PC Usage Procedures

In order to ensure compliance with local, state, and federal computer crime laws, copyright laws, and to prevent inappropriate and non-company related use of AISD Communication and Information Systems by AISD Employees and to protect AISD from being victimized by malicious acts of compromising organization assets, the following is AISD's regulations on the use of AISD Communication and Information Systems and/or Internet:

1. AISD Communication and Information Systems and/or Internet are not to be used in a way that may be disruptive, illegal, offensive to others, or harmful to morale, including unauthorized access and other unlawful activities. AISD maintains a process for monitoring employee usage of AISD's Communication and Information Systems and/or Internet and will fully investigate suspected abuse. Employees are responsible for preventing misuse of their computer equipment and should take reasonable and appropriate precautions to protect AISD's systems, including securing their computers (locking when not in use and securing when stored or transported.) AISD Communication and Information Systems and/or Internet are not to be used as personal bulletin services. AISD Communication and Information Systems and/or Internet are not to be used to transmit or knowingly receive vulgar, profane, insulting, or offensive messages, including racial, sexual slurs or jokes, harassing or threatening messages or pornography. AISD is required to comply with all applicable federal laws and will report to authorities any individual accessing, transmitting, or knowingly receiving illegal information through an AISD Communications and Information System and/or Internet, including child pornography and illegally obtained software.
2. Employees using AISD Communication and Information Systems and/or Internet are to use such services in a professional manner so as not to damage the reputation of the organization. AISD Communication and Information Systems and/or Internet are to be used in compliance with AISD's standard of business ethics and professional conduct. AISD may choose to hold an employee liable for any damage to AISD's reputation or systems as a result of an employee's misuse or AISD's Communication and Information Systems and/or Internet.
3. Files that are downloaded from the Internet must be scanned with up-to-date virus detection software before installation or executions. All appropriate precautions must be taken to detect for a virus and, if necessary, to prevent its spread. The introduction of viruses, or malicious tampering with any computer system, is expressly prohibited. Questions on how to scan with virus detection software should be directed to the Help Desk. All identified viruses must be reported to the Help Desk.
4. Unauthorized employees shall not place company confidential or proprietary material (including but not limited to copyrighted software, internal correspondence, or e-mail) on any publicly accessible Internet computer. Sensitive material transferred over the Internet may be at risk of detection by a third party without precautions. Employees must exercise caution and care when transferring such material in any form. AISD confidential information is not to be transmitted or forwarded to outside individuals or companies not authorized to receive the information or AISD employees who do not have a business need for the information.. Alternate Internet Service Provider (ISP)

connections to AISD's internal network are not permitted. Examples of ISP's are America Online, Microsoft Network, Internet America, etc.

5. Unless otherwise noted, all software on the Internet should be considered copyrighted work. Therefore, employees are prohibited from downloading software and/or modifying any such files without consulting the Help Desk. Employees are required to adhere to all licensing and copyright laws and cannot use electronic communications systems to send (upload) or receive (download) copyrighted materials including software.
6. AISD reserves the right to restrict access to any materials that are inappropriate to minors and/or illegal materials. AISD also reserves the right to restrict access to and/or filter any type of direct communications (including electronic mail and chat rooms) that are outside of the AISD Communication and Information Systems and/or Internet.
7. Vandalism is prohibited. Any malicious attempt to harm or destroy AISD equipment or materials, data of another user of the AISD's system, or any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to compromise, degrade, or disrupt system performance may be viewed as violations of AISD policies and administrative regulations and, possibly, as criminal activity under applicable state and federal laws. This includes, but is not limited to, the uploading or creating of computer viruses.
8. AISD Communication and Information Systems and/or Internet are AISD property and are not private. Employees do not have a personal privacy right in any material created, stored, received or sent in or through AISD Communication and Information Systems and/or Internet. By using AISD Communication and Information Systems and/or Internet, all employees knowingly and voluntarily consent of their usage of these systems being monitored and acknowledge and agree to AISD's right to conduct such monitoring. AISD, in its sole discretion, reserves the right to access, monitor, copy, transcribe, forward, download, capture, and/or disclose all communications sent via any AISD Communication and Information System and/or Internet at any time, with or without prior notice. Violations of AISD's procedures on use of its Communications and Information Systems and/or Internet may result in disciplinary action up to and including termination of employment or dismissal.

Internet Safety Procedures

AISD currently utilizes DeepNines for monitoring and filtering Internet traffic. Each year we evaluate whether to upgrade or purchase new and other products to give the organization and the services we provide the protection needed. Internet filtering blocks or filters Internet access. It protects against access by adults and minors to visual depictions that are obscene, child pornography, or - with respect to use of computers with internet access by minors – harmful to minors. It may be disabled for adults engaged in bonafide research or other lawful purposes. It includes monitoring the online activities of minors.

AISD internet filtering prevents access by minors to inappropriate matter on the Internet and World Wide Web. It also monitors electronic mail, chat rooms, and other forms of direct electronic communications and unauthorized accessing and other unlawful activities online. AISD is committed to the education of minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber-bullying awareness and response.