



815. ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET,  
ELECTRONIC COMMUNICATIONS, AND INFORMATION SYSTEMS - Pg. 2

<p>P.L. 106-554 Sec. 1711, 1721</p>	<p>and/or administer appropriate disciplinary action. The district will cooperate to the extent legally required with the ISP, local, state and federal officials in any investigation concerning or related to the misuse of the CIS systems.</p> <p>It is often necessary to access user accounts in order to perform routine maintenance and security tasks; system administrators have the right to access by interception, and the stored communication of user accounts for any reason in order to uphold this policy and to maintain the system. Users have no privacy expectation in the contents of their personal files or any of their use of the district's CIS systems. The district reserves the right to monitor, track, log and access CIS system use and to monitor and allocate fileserver space.</p> <p>The school district reserves the right to restrict access to any Internet sites or functions it may deem inappropriate through software blocking or general policy. The district will use specific technology to accomplish this task as defined on the district web site for technology policies and procedures. Specifically, the school district operates and enforces technology protection measure(s) that block or filter online activities pursuant to the Children's Internet Protection Act. Programs or services being utilized to block access shall be identified on the district's web site.</p> <p>The filter may be disabled by the network administrator at the workstation level use by an adult administrator or teacher for bona fide research or other lawful purposes. The filter may not be disabled for use by students or other minors for any reason.</p> <p>The district reserves the right to restrict or limit usage of lower priority CIS systems and computer uses when network and computing requirements exceed available capacity.</p> <p>The school district additionally reserves the right to:</p> <ol style="list-style-type: none"><li>1. Determine which CIS system services will be provided through school district resources.</li><li>2. View and monitor network traffic, file server space, processor, and system utilization, and all applications provided through the network and communications systems, including e-mail.</li><li>3. Remove excess e-mail or files taking up an inordinate amount of fileserver disk space after a reasonable time.</li></ol>
---	---

815. ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET,  
ELECTRONIC COMMUNICATIONS, AND INFORMATION SYSTEMS - Pg. 3

<p>3. Delegation of Responsibility</p> <p>4. Guidelines</p>	<p>4. Revoke user privileges, remove user accounts, or refer to legal authorities when violation of this and any other applicable district policies occur or state or federal law is violated, including, but not limited to, those governing network use, copyright, security, privacy, employment, and destruction of school district resources and equipment.</p> <p>The Director of Technology Services and/or designee will serve as the coordinator to oversee the district's CIS systems and will interpret and enforce this policy.</p> <p><u>Parental Notification And Responsibility</u></p> <p>Parents/Guardians shall be informed of the policy at the time of student registration for school. This policy shall be included in the Student Code of Conduct and shall be available on the district web site.</p> <p><u>School District Limitation Of Liability</u></p> <p>The district makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the district's CIS systems will be error-free or without defect. The school district does not warrant the effectiveness of Internet filtering.</p> <p><u>Prohibitions</u></p> <p>The use of the school district's CIS systems for illegal, inappropriate, unacceptable, or unethical purposes or for sending, receiving, viewing or downloading visual depictions of obscenity, child pornography or material that is harmful to minors is prohibited. The terms child pornography, obscene, and harmful to minors shall have definitions set forth in the Child Internet Protection Act, Act 226 of 2003.</p> <p>Access and Security Prohibitions -</p> <p>Users must immediately notify the Director of Technology Services and/or designee if they have identified a possible security problem.</p> <p>Operational Prohibitions -</p> <p>Sharing of passwords or interfering with or disrupting the CIS systems, network accounts, services or equipment of others, including, but not limited to, propagating computer "worms" and "viruses", Trojan Horse and trapdoor program code, the sending of electronic chain mail, distasteful jokes, and the inappropriate sending of "broadcast" messages to large numbers of individuals or hosts.</p>
---	--

Incidental Personal Use -

Personal use must comply with this policy and all other school district policies, procedures and rules, as well as ISP, local, state and federal laws and may not interfere with the employee's job duties and performance, with system operations, or with other system users, and must not damage the district's CIS systems. Under no circumstances should the user believe their use is private. The school district reserves the right to monitor, track, access, and log the use of its CIS systems at any time.

Content Guidelines

Information electronically published on the district's CIS systems shall be subject to the district technology guidelines posted on the web site under technology policies and procedures.

Due Process

The district shall cooperate with the school district's ISP, local, state, and federal officials to the extent legally required in investigations concerning or relating to any illegal activities conducted through or relating to the school district's CIS systems.

If students or employees possess due process rights for discipline resulting from the violation of this policy, they will be provided such rights.

The district may terminate the account privileges by providing notice to the user.

Search And Seizure

Users' violations of this policy, any other district policy, or the law may be discovered by routine maintenance and monitoring of the school district system, or any method stated in this policy, or pursuant to any legal means.

The district reserves the right to monitor, track, log and access any electronic communications, including but not limited to, Internet access and e-mails at any time for any reason. Users shall not have any expectation of privacy in their use of the school district's CIS systems, and other school district technology, even when used for personal reasons. Further, the district reserves the right, but not the obligation, to access any personal technology device of users brought onto the school district's premises or at school district events, or connected to the school district network, containing district programs or district or student data (including images, files, and other information) to ensure compliance with this policy and other district policies, to protect the school district's resources, and to comply with the law.

815. ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET,  
ELECTRONIC COMMUNICATIONS, AND INFORMATION SYSTEMS - Pg. 5

Pol. 814	<p>Everything that users place in their personal files should be written as if a third party will review it.</p> <p><u>Copyright Infringement And Plagiarism</u></p> <p>Use of the CIS systems for copyright infringement and plagiarism is prohibited.</p> <p><u>Selection Of Material</u></p> <p>Board policies on the selection of materials will govern use of the district's CIS systems.</p> <p>When using the Internet for class activities, teachers will select material that is appropriate in light of the age of the students and that is relevant to the course objectives. Teachers shall preview the materials and web sites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the web site. Teachers will provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Teachers shall assist their students in developing the critical thinking skills necessary to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.</p> <p>A student or employee who claims that this policy is denying him/her access to material which is not prohibited by this policy shall have the right to review by filing a written request with the Director of Technology Services.</p> <p>The written request shall specifically describe the material which cannot be accessed, and the reasoning supporting the claim that the material is not prohibited. The Director of Technology Services shall issue a written decision resolving the claim within ten (10) days of receipt of the written request.</p> <p>If the student or employee is dissatisfied with the decision, s/he may request further review by the Superintendent by filing a written request with the Superintendent within ten (10) days after the written decision is issued. The Superintendent shall issue a written decision within ten (10) days after the written request is received, and this decision shall constitute the final decision of the district.</p>
----------	---

815. ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET,  
ELECTRONIC COMMUNICATIONS, AND INFORMATION SYSTEMS - Pg. 6

<p>18 Pa. C.S.A. Sec. 5703</p>	<p><u>School District Web Site</u></p> <p>The district shall establish and maintain a web site and will develop and modify its web pages to present information about the school district under the direction of the Director of Technology Services. Publishers must comply with the district's web site development policy.</p> <p><u>Safety And Privacy</u></p> <p>To the extent legally required, users of the district's CIS systems shall be protected from harassment or commercially unsolicited electronic communication. Any user who receives threatening or unwelcome communications must immediately take them to the Director of Technology Services and/or designee.</p> <p>Users will not post personal contact information about themselves or other people on the CIS systems. The user may not steal another's identity in any way, may not use spyware, parasiteware, cookies, or use school district or personal employee technology or resources in any way to invade one's privacy.</p> <p>Additionally, the user may not disclose, use or disseminate confidential and personal information about students or employees (examples include, but are not limited to, using a cell phone with camera and Internet access to take pictures of anything, including but not limited to, persons, places, and documents relevant to the district, saving, storing and sending the image with or without text or disclosing them by any means, including but not limited to, print and electronic matter; revealing student grades, social security numbers, home addresses, telephone numbers, school addresses, work addresses, credit card numbers, health and financial information, evaluations, psychological reports, educational records, reports, and resumes or other information relevant to seeking employment at the district unless legitimately authorized to do so).</p> <p>Student users shall not meet face to face with someone they have met online unless they have parental consent.</p> <p><u>Consequences For Inappropriate, Unauthorized And Illegal Use</u></p> <p>General rules for behavior, ethics, and communications apply when using the CIS systems and information, in addition to the stipulations of this policy. Violations of this policy or other policies, or unlawful use of the CIS systems may result in loss of CIS access and a variety of other disciplinary actions, including but not limited to, warnings, usage restrictions, loss of privileges, position reassignment, oral or written reprimands, suspensions (with or without pay for employees), dismissal, expulsions,</p>
------------------------------------	--

815. ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET,  
ELECTRONIC COMMUNICATIONS, AND INFORMATION SYSTEMS - Pg. 7

<p>P.L. 94-553 Sec. 107 P.L. 106-554 Sec. 1711, 1721, 1732</p> <p>20 U.S.C. Sec. 6777</p> <p>PA Code Title 22 Sec. 403.1</p> <p>School Code 24 P.S. Sec. 4601 et seq</p> <p>Board Policy 814</p>	<p>and/or legal proceedings on a case-by-case basis. The district administrative staff, along with the system administrator, shall deem what is appropriate and inappropriate use.</p> <p><u>Etiquette</u></p> <p>Users are expected to abide by the generally accepted rules of network etiquette as posted on the district web site.</p> <p><u>Disclaimer</u></p> <p>The school district makes no warranties of any kind, whether expressed or implied, for the service it is providing. The district is not responsible, and will not be responsible, for any damages, including loss of data resulting from delays, nondeliveries, missed deliveries, or service interruption. Use of any information obtained through the use of the school district's computers is at the user's risk. The district disclaims responsibility for the accuracy or quality of information obtained through the Internet or e-mail.</p>
--	--