

CIPA POLICY & STUDENT USE AGREEMENT

The Children's Internet Protection Act ("CIPA"), 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 ("NCIPA") which addresses the broader issues of electronic messaging, disclosure of personal information of minors, and unlawful online activities. The Protecting Children in the 21st Century Act, enacted October 10, 2008, adds an additional Internet Safety Policy requirement covering the education of minors about appropriate online behavior.

Freedom Academy purchased a SG5 firewall from Juniper Networks to protect our network. This Internet appliance is outfitted with a content filter that blocks inappropriate sites. Juniper maintains and regularly updates its content filtering database. It automatically passes those updates through to our firewall device. Each year, to remain compliant with CIPA regulations, we renew our content filtering subscription and block access to inappropriate sites. In addition we have posted a copy of our **Internet Use Policy** on our school Web site. The CIPA Requirement and district policy is included below for reference.

CIPA Requirements:

"Undertaking such actions" refers to actions related to implementation of the CIPA requirements that should be in place for Year 2005. These requirements are:

1. Technology Protection Measure

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, 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 bona fide research or other lawful purposes. For schools, the policy must also include monitoring the online activities of minors.

2. Internet Safety Policy

The Internet Safety Policy must address the following issues:

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 so-called "hacking," and other unlawful activities by minors online; unauthorized disclosure, use, and dissemination of personal information regarding minors; and measures designed to restrict minors' access to materials harmful to minors.

3. Public Notice and Hearing

The authority with responsibility for administration of the school or library must provide reasonable public notice and hold at least one public hearing to address a proposed Technology Protection Measure and Internet Safety Policy.

Freedom Academy Student Technology Use Policy

Student Use of Computers, Local area network, and Internet

School-Provided Access to Electronic Information, Services, and Networks

Internet access is available to the students and faculty of Freedom Academy. Through its computer network, Freedom Academy is connected with thousands of computers all over the world. Users may have access to information ranging from different cultures, science related issues, music, politics, and access to many university library catalogs. These are just some of the areas users may be able to explore through the computer network.

Students utilizing school-provided Internet access are responsible for good behavior on-line, just as they are in a classroom or other area of the school. The same general rules for behavior and communications apply. The purpose of Freedom Academy provided Internet access is to facilitate communications in support of research and education.

To remain eligible as users, students' use must be in support of and consistent with the educational objectives of Freedom Academy. Access is a privilege, not a right. Access entails responsibility.

Inappropriate Sites

The use of the District network and the Internet is for educational purposes only. All sites containing pornography or sexually explicit materials (written or pictured) are off limits to users

Privacy/Confidentiality

Users should have no expectation of privacy or confidentiality in the content of electronic communications or other computer files sent and received on the school computer network or stored in his/her directory. The school computer network's system operator, or other school employees, may at any time review the subject, content, and appropriateness of electronic communications or other computer files and remove them if warranted. Any violation of District rules will be reported to school administrators.

Personal Information

When sending electronic messages, students shall not include information that could identify themselves, other students, or staff. Examples of identifying information include last names, addresses, and phone numbers. Users' network passwords are provided for their personal use. Users should not share their password with anyone. Users should not log into the network with another user's login name and password. If a user suspects someone has discovered their password, they should change it or have it changed immediately. Users shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users.

Copyright

Users shall not:

1. Copy and forward;
 2. Copy and download; or
 3. Copy and upload to the network or Internet server any copyrighted material, without approval by the computer system operator, a teacher, or other school administrator.
- Copyrighted material is anything created by someone else. Examples include, but are not limited to reports, articles, pictures, music, or software. Do not plagiarize or steal others' work.

