

Enid Public Schools *Internet Protection Guidelines*

Students are responsible for good behavior on school computer networks just as they are in a classroom or a school hallway. Communications on the network are often public in nature. General school and district rules for behavior and communications apply.

The network is provided for students to conduct research. Individual users of the district computer networks are responsible for their behavior and communications over those networks. Users will comply with the standards established by the district. Also, the district has purchased software for Internet content filtering. This allows students to explore the Internet in relative safety.

Network storage areas may be treated like school lockers. The technology director and network administrator may review files and communications to maintain system integrity and insure that users are using the system responsibly. Users should have no expectations of privacy in their electronic files stored on Enid Public School District computers.

Enid Public Schools intends to provide access to the Internet as a tool for educational activities. During school, teachers of younger students will guide them toward appropriate materials. Outside of school, families bear the same responsibility for such guidance as they exercise with other information sources such as television, telephones, radio and movies. Students using the district network are not permitted to do the following:

- Access offensive messages or pictures.
- Use obscene or defamatory language.
- Harass, insult, defame or attack others.
- Damage computers, altering computer systems or computer networks.

Enid Public Schools CIPA - Children's Internet Protection Act, 2001

The Internet is an important teaching tool used in Enid Public Schools classrooms and libraries. The Internet can, however, provide students with access to inappropriate material.

Federal law (*CIPA - Children's Internet Protection Act, 2001*) requires school districts to use "filtering" software that attempts to block access to visual depictions and descriptions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by CIPA and as determined by the District. Therefore, all Internet access is filtered for minors and adults on computers with Internet access provided by the District. In fact, NOT doing so would result in the loss of millions of dollars to the District in federal and state funding (E-rate, Title II Part D, TEA technology grants).

If users need a site unblocked for instructional or operational purposes, or if users feel a particular site is inappropriate and needs to be blocked, users should contact your building principal and the principal will contact the "Helpdesk" <http://www.enidpublicschools.org/workorderform2.htm> (Be sure to include the URL / Internet address.).

Websense is the Internet filtering program used by the filter. "Blocking" categories are reviewed at least annually by the District. Currently, *Websense* is configured to block websites in which the **content** is categorized / classified as:

Adult Material	Adult Content
Nudity Sex (not Sex Education)	Lingerie and Swimsuit
Abused Drugs	Marijuana
MP3 and Audio Download Services	Gambling
Games	Illegal or Questionable Hacking
Proxy Avoidance	Weapons
Sport Hunting and Gun Clubs	Pay to Surf Internet Auctions
Web Chat	Web-based Email
Militancy and Extremist Racism and Hate	Non-Traditional Religions and Occult and Folklore
Alcohol and Tobacco	Gay and Lesbian or Bisexual Interest
Personals and Dating	Tasteless Violence
Advertisements	Malicious Websites
Spyware	Keyloggers
Phishing and Other Frauds	

The District has also blocked access to image search engines, such as Google Images, to reduce the possibility of students coming across inappropriate pictures while doing searches on the Internet.