

## **Internet Safety**

### To Our Staff

Access to the Beeville ISD network and Internet are provided to you as tools for conducting school business. Appropriate access and use of these resources is **YOUR** responsibility when you use them, regardless of your job classification. The smooth operation of these technologies depends upon your proper and responsible conduct in accordance with district policies.

The Internet is an important teaching tool used in Beeville ISD 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. For this reason, Beeville ISD uses "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 the federal Children's Internet Protection Act. **No filtering software product is foolproof.**

The current filtering software comes with a programmed list of blocked sites. The list of blocked sites is updated daily. In addition, key district personnel have the ability to add sites to the blocked-sites list, and also to allow access to a blocked site upon approval by your campus administrator. If you need a site unblocked for instructional or operational purposes, or if you feel a particular site is inappropriate and needs to be blocked, contact your principal who will forward the request to the Technology Director. Allow at least 24 hours for the change to occur.

The categories Lightspeed currently blocks are:

- Adult material
- Adult art
- Adult bodyart
- Adult games
- Adult language
- Adult lifestyles
- Alcohol
- Drugs
- Gambling
- Porn
- Child porn
- International porn sites (German, Spanish, etc.)
- Suspicious
- Suspicious Java Script

- Violence
- Hate violence
- Weapons violence
- Forums
- Blogs
- Instant Messaging
- Newsgroup forums
- Peer to peer (p2p) forums
- Personal forums (personal ads, etc.)
- Parked (sites where you pay per click)
- Security risk sites
- Computer hacking
- Phishing
- Proxy (sites where you can get around the Internet filter)
- Spyware
- Virus security
- Security warez (sites promoting illegal access and sharing of software and other copyrighted material)
- Shopping
- Automobile
- Finance
- Jobs
- Real Estate
- Games
- Lifestyles
- Kids and Teens Chat
- Plagiarism
- Audio-video
- Hobbies
- Humor
- Music
- Sports
- Fantasy Sports
- Martial Arts

For those of you with students under your supervision, it is important to "lay the ground rules" with students before beginning any classroom projects involving the Internet and the network. Actively monitor students as they use the computer equipment, and help them become ethical and responsible users of the Internet and related technologies.

Be conscious of the physical security of your equipment, especially if you work in an area visited often by persons from outside your Department or from the public. Lock doors to offices when not used or during off-hours. Maintain physical security of any portable computer equipment such as laptops or notebooks.