

COPYRIGHTED MATERIALS

Policy EFE

Employees are expected to comply with the provisions of copyright law relating to the unauthorized use, reproduction, distribution, performance, or display of copyrighted materials (i.e., printed materials, videos, computer data and programs, etc.). Rented videotapes are to be used in the classroom for educational purposes only. Duplication or back-up of computer programs and data must be made within the provisions of the purchase agreement.

COMPUTER USE, DATA MANAGEMENT AND INTERNET FILTERING SOFTWARE

Policy CQ (Local)

Employees are expected to follow the acceptable use policy when accessing district computers and the Internet. Violations of the acceptable use policy may be identified as acts of misconduct with penalties. Individuals who continuously attempt to break through the Internet filter, whether successful or not, are subject to disciplinary action.

BISD TECHNOLOGY ACCEPTABLE USE GUIDELINES FOR EMPLOYEES

Policy CQ (Local)

Acceptable Use

Birdville ISD's technology resources will be used only for learning, teaching and administrative purposes consistent with the district's mission and goals. All district technology training will emphasize the ethical use of district technology resources and the acceptable use guidelines. Commercial use of the district's technology resources is strictly prohibited.

Definition of District Technology Resources

The district's computer systems and networks are any configuration of hardware and software. The systems and networks include all the computer hardware, operating system software, application software, stored text, and data files. This includes electronic mail, local databases, externally accessed databases (such as the internet), CD-ROM, optical media, clip art, digital images, digitized information, telecommunications devices and all new technologies as they become available. The district reserves the right to monitor all technology resource activity.

The use of the network is a privilege that may be revoked by network administrators or authorized faculty designees at any time for violation of district policy and/or administrative regulations regarding acceptable use. The district shall not be liable for the inappropriate use of electronic communication resources, violations of copyright restrictions, mistakes, negligence, or costs incurred by users. The district will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the district's computer systems and networks.

Blogs, Podcasts, Forums and Wikis

Inappropriate use of district computers to post personal blogs, forums, wiki's or podcasts is prohibited. Posting any student or teacher created blog or podcast that is not directly related to and in support of the BISD approved curriculum is prohibited.

Consequences of Improper Use

The district's technology resources may not be used for improper, unethical, or illegal purposes, in support of illegal activities, or for any other activity prohibited by district policy. Users may not use another person's network account. Any district network user identified as a security risk or as having violated district and/or campus computer-use guidelines may be denied access to the district's network or may result in disciplinary actions.

E-mail

The software and hardware that provides e-mail capabilities is publicly funded. For that reason, it should not be considered a private, personal form of communication. The Open Records Act governs the contents of any electronic communication. BISD abides and cooperates with any legal request for access.

It is the policy of the district that information transmitted by e-mail be retained in accordance with the department's records retention schedule by the legal custodian (originator or individual to whom the message is addressed) of the e-mail message. As the legal custodian, users must print out and save paper copies of important documents or archive them in personal folders on their hard drives or other storage devices in compliance with the retention requirements of the Open Records Act.

BISD e-mail servers are provided to facilitate the delivery of e-mail. Information is backed up as a safety measure in case of system failure or unlawful tampering (“hacking”). Network Support Services deletes all e-mail messages in early July of each school year as part of the routine maintenance of the e-mail system.

Forgery Prohibited

Forgery or attempted forgery of e-mail messages is prohibited. Attempts to read, delete, copy, or modify the e-mail of other users or deliberate interference with the ability of other users to send/receive e-mail is prohibited.

Hardware

All hardware purchases should be for those items that are approved by the TIMS department and listed in the current technology bid because we have maintenance agreements on those items.

Information Content/Third Party Supplied Information

System users and parents of students with access to the district’s system should be aware that use of the system may inadvertently provide access to other electronic communications systems outside the district’s networks that may contain inaccurate and/or objectionable material. The district will maintain Internet filtering to attempt to minimize the access to objectionable material. Any attempt to circumvent the filtering software will be viewed as an attempt to disrupt the system and constitutes inappropriate use. Non-business related purchases made over the Internet are prohibited. Internet access may not be used for personal gain.

An employee who knowingly brings or transmits prohibited, obscene, or pornographic materials into the school’s electronic environment will be subject to disciplinary action in accordance with district policies. This could result in termination of employment.

Maintenance of Local hard Drives

NOTE: BISD faculty and staff are personally responsible for making backups of any data files that you store on your local hard drive.

All district computers (desktop and laptops) must have auto-updating virus protection.

NOTE: Electronic files created, sent, received, or stored on computers owned, leased, administered, or otherwise under the custody and control of Birdville ISD are the property of Birdville ISD. These files are not private and may be accessed at any time by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 201.13(b), Information Resource Standards and may be subject to the Open Records Act.

Network Etiquette

District network users are expected to be polite and use appropriate language. Users should not misrepresent their identity, transmit obscene messages or pictures, reveal personal addresses or phone numbers, or use the network in a way that would disrupt the use of the network by others.

Software

No software should, or will, be installed without documentation that shows the software purchase has gone through an approval process that includes the TIMS department.

Software purchased for Birdville ISD may not be installed on home computers. Programs brought from home are not allowed to be installed on BISD computers. The cost of any fines levied upon the district due to the aforementioned behavior will be passed on to the individuals responsible for the illegal software. BISD reserves the right to remove any non-business related software or files from any computer without notification. Examples of non-business related software or files include, but are not limited to games, instant messengers, pop e-mail, music files, image files, freeware and shareware.

Copyrighted software or data may not be placed on any computer connected to the district’s network without permission from the holder of the copyright. Only the owner(s) or individuals the owner specifically authorizes may upload copyrighted material to the network.

Telecommunications

The use of all district provided telecommunications equipment to include but not limited to desk phones, cell phones, pagers, walkie-talkies, etc. is a privilege not a right. These technologies have been publicly funded. For that reason, they should not be considered a private, personal form of communication. Personal use is inappropriate. The contents of any communication of this type are governed by the Network Access General Use Policy. All terms that are covered in the policy including user responsibilities and consequences for policy violations, apply to use of these devices.