

# **Bells Independent School District Internet Safety Policy**

## **Introduction**

It is the policy of Bells ISD to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

## **Definitions**

See key terms are as defined in the Children's Internet Protection Act\* below.

## **Access to Inappropriate Material**

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information.

Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

## **Inappropriate Network Usage**

To the extent practical, steps shall be taken to promote the safety and security of users of the Bells Independent School District online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

## **Education, Supervision and Monitoring**

It shall be the responsibility of all members of the Bells Independent School District staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21<sup>st</sup> Century Act. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Technology Director or designated representatives.

All people using communication systems within the School District shall refrain from accessing material, which is pornographic, harassing, advocates violence, or has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile or offensive environment within the School District. All electronic information systems shall have reasonable devices in place to prevent unauthorized use of such systems and to prevent intended and unintended access to inappropriate Internet sites by any student, employee, or visitor. Inappropriate sites are those, which contain material, which is prohibited by this Policy. Violations of this section will result in disciplinary action up to expulsion for students, dismissal for employees, and ejection and barring of visitors.

## **Adoption**

The Board of Bells Independent School District adopted this updated Internet Safety Policy at a public meeting, following normal public notice, on October 18, 2010.

*\*CIPA definitions of terms:*

*TECHNOLOGY PROTECTION MEASURE. The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:*

- 1. "Obscene" as that term is defined in section 1460 of title 18, United States Code;*
- 2. "Child Pornography" as that term is defined in section 2256 of title 18, United States Code; or*
- 3. "Harmful to minors"*

*HARMFUL TO MINORS. The term "Harmful to Minors" means any picture, image, graphic image file, or other visual depiction that:*

- 1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;*
- 2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and*
- 3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.*

*SEXUAL ACT; SEXUAL CONTACT. The terms "Sexual Act" and "Sexual Contact" have the meanings given such terms in section 2246 of title 18, United States Code.*

# **Guidelines for Acceptable Use of Bells Independent School District Technology Resources**

The Bells Independent School District provides technology resources to its students and staff for educational and administrative purposes. The goal in providing these resources is to promote educational excellence in the Bells schools by facilitating resource sharing, innovation, and communication with the support and supervision of parents, teachers, and support staff. The use of these technology resources is a privilege, not a right.

With access to computers and people all over the world comes the potential availability of material that may not be considered to be of educational value in the context of the school setting. Bells ISD firmly believes that the value of information, interaction, and research capabilities available outweighs the possibility that users may obtain material that is not consistent with the educational goals of the district.

Proper behavior, as it relates to the use of computers, is no different than proper behavior in all other aspects of Bells ISD activities. All users are expected to use the computers and computer networks in a responsible, ethical, and polite manner. This document is intended to clarify those expectations as they apply to computer and network usage and is consistent with District Policy CQ (Local).

## **Definition of District Technology Resources**

The District's computer systems and networks are any configuration of hardware and software. The systems and network include all of 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, communications technologies, and new technologies as they become available. The District reserves the right to monitor all technology resource activity.

## **Acceptable Use**

The District's technology resources will be used only for learning, teaching, and administrative purposes consistent with the District's mission and goals.

The District will make training available to all users. All training in the use of the District's system will emphasize the ethical use of this resource.

Software of external data may not be placed on any computer, whether stand-alone or networked to the District's system, without permission from the Superintendent or designee.

Other issues applicable to acceptable use are:

1. Copyright: All users are expected to follow existing copyright laws, copies of which may be found in the BHS library.

2. Supervision and permission: Student use of the computers and computer network is only allowed when supervised or granted permission by a staff member.
3. Attempting to log on or logging on to a computer or email system by using another's password is prohibited: Assisting others in violating this rule by sharing information or passwords is unacceptable.
4. Improper use of any computer or the network is prohibited. This includes the following:
  - Using racist, profane, or obscene language or materials
  - Using the network for financial gain, political or commercial activity
  - Attempting to or harming equipment, materials, or data
  - Attempting to or sending anonymous messages of any kind
  - Using the network to access material that the school district considers inappropriate
  - Knowingly placing a computer virus on a computer or the network
  - Using the network to provide addresses or other personal information that others may use inappropriately
  - Accessing of information resources, files and documents of another user without their permission

## **System Access**

Access to the District's network systems will be governed as follows:

1. Students will have access to the District's resources for class assignments and research with their teacher's permission and/or supervision.
2. Teachers with accounts will be required to maintain password confidentiality by not sharing the password with students or others.
3. With the approval of the immediate supervisor, district employees will be granted access to the District's system.
4. Any system user identified as a security risk or having violated District Acceptable Use Guidelines may be denied access to the District's system. Other consequences may also be assigned.

## **Individual User Responsibilities**

The following standards will apply to all users of the District's computer network system:

1. The individual in whose name a system account is issued will be responsible at all times for its proper use.
2. The system may not be used for illegal purpose, in support of illegal activities, or for any other activity prohibited by district guidelines.
3. System users may not use another person's system account without written permission from the campus coordinator or principal, as appropriate.
4. System users assigned email accounts are asked to purge electronic mail or outdated files on a regular basis.
5. System users are responsible for making sure they do not violate any copyright laws.

## **Vandalism Prohibited**

Any malicious attempt to harm or destroy District equipment or materials, data of another user of the District's system, or any of the agencies or other networks to which the District has access is prohibited. Deliberate attempts to degrade or disrupt system performance may be viewed as violations of district guidelines and, possibly, as criminal activity under applicable state and federal laws, including the Texas Penal Code, Computer Crimes, Chapter 13. This includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above will result in the cancellation of system use privileges and possible prosecution and will require restitution for costs associated with system restoration, hardware, or software.

## **Forgery Prohibited**

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

## **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 provide access to other electronic communications systems outside the District's network that may contain inaccurate and/or objectionable material.

A student bringing prohibited materials into the school's electronic environment will be subject to a suspension and/or a revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Student Code of Conduct. An employee knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies.

## **Network Etiquette**

System users are expected to observe the following network etiquette:

1. Use appropriate language: swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited.
2. Pretending to be someone else when sending/receiving messages is prohibited.
3. Transmitting obscene messages or pictures is prohibited.
4. Revealing such personal information as addresses or phone numbers of users or others is prohibited.
5. Using the network in such a way that would disrupt the use of the network by other users is prohibited.
6. Be considerate. For example, messages typed in capital letters are the computer equivalent of shouting and are considered rude.

## **Termination/Revocation of System User Account**

The District may suspend or revoke a system user's access to the District's system upon violation of District policy and/or administrative regulations regarding acceptable use.

Termination of an employee's account or of a student's access will be effective on the date the principal or campus coordinator receives notice of user withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

## **Consequences of Improper Use**

Improper or unethical use may result in disciplinary actions consistent with the existing Student Discipline Policy and, if appropriate, the Texas Penal Code, Computer Crimes, Chapter 33, or other state and federal laws. This may also require restitution for costs associated with system restoration, hardware, or software.

## **Monitored Use**

Electronic mail transmissions and other use of the electronic communications system by students and employees shall not be considered confidential and may be monitored at any time by designated District staff to ensure appropriate use for educational or administrative purposes.

## **Disclaimer of Liability**

The District shall not be liable for users' inappropriate use of electronic communication resources or violations of copyright restrictions, users' mistakes or negligence, or costs incurred by users. The District shall not be responsible for ensuring the accuracy or usability of any information found on the Internet.

## **Disclaimer**

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether expressed or implied, including, without limitation, those of fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District uses a variety of vendor supplied hardware and software. Therefore, the District does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the user's requirements. Neither does the District warrant that the system will be uninterrupted or error-free, nor that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third party individuals in the system are those of the providers and not necessarily the District.

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.