

**Computer, Electronic Communications Systems and Network Access  
Acceptable Use Policy and Internet Safety Policy for Students and Employees  
for Bosqueville Independent School District Technology Resources**

The Bosqueville Independent School District provides technology resources to its students and staff for educational and administrative purposes. The use of these technology resources is a privilege, not a right. Bosqueville ISD complies with Federal Regulations regarding Internet filtering in order to limit user access to inappropriate content. All users are expected to use the computers and computer networks in a responsible, ethical, and polite manner

**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 of the computer hardware, operating system software, application software, stored text, and data files. This includes but is not limited to electronic mail, local databases, externally accessed databases (i.e. the Internet), CD-ROM, optical media, clip art, digital images, digitized information, communications technologies, and new technologies as they become available. The District will at its own discretion monitor any technology resource activity without further notice to the end user.

**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 email system should not be used for mass mailings except for official school business. Personal e-mail should not impede the conduct of district business. Employee time may be restricted by Campus Administrator.

The District will make training available to all users in the proper use of the system and will make copies of acceptable use guidelines available to all users. All training in the use of the District's system will emphasize the ethical use of this resource. BISD will educate the users on digital citizenship, digital etiquette, security, cyber bullying, etc.

**SYSTEM ACCESS**

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

1. BISD users will have access to the District's resources for class assignments and research with their teacher's permission and supervision.
2. Teachers with accounts will be required to maintain password confidentiality by not sharing passwords.
3. Teachers are not allowed to provide student access through the teacher's account.
4. Any system user identified as a security risk or having violated District Acceptable Use Policies may be denied access to the District's system. Other consequences may also be imposed.
5. Any system user having been denied access rights may be reinstated with a limited access account to reduce the level of security risk to the system. Limits on this type of account may include time limitations, home directory limitations, station access limitations, file access restrictions, and a revocation of Internet access privileges.
6. 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.
7. Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

## **CAMPUS LEVEL RESPONSIBILITIES**

The campus principal or designee will:

1. Be responsible for disseminating, collecting signed permission forms, and enforcing the District Acceptable Use Policy for the District's system at the campus level.
2. Ensure that employees supervising students who use the District's systems provide information emphasizing the appropriate and ethical use of this resource.

## **INDIVIDUAL USER RESPONSIBILITIES**

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

1. The individual in whose name a system account is issued will be responsible for its proper use at all times.
2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District Policies.
3. System users may not use another person's system account to access computer or network resources.
4. System users are required to delete outdated electronic mail or files on a regular basis. A limit of 250 megabytes will be maintained for all electronic mail accounts. Also, all sent items will be deleted after 120 days and all trash will be deleted after 120 days.
5. System users are responsible for saving or archiving any critical items sent or received within the electronic mail system. The Technology department is not responsible for saving, backing up, or archiving electronic mail due to the high storage demands placed on the system.
6. System users will be responsible for the care of their systems. Maintenance issues must be reported to the Technology Department in a timely manner.
7. System users will be responsible for following all copyright laws.
8. 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 is the responsibility of all members of the BISD staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Technology Director or designated representatives. BISD will provide age appropriate training for students who use the BISD Internet facilities. The training provided will be designed to promote Bosqueville's commitment to:

- a. The standards and acceptable use of Internet services as set forth in the BISD Internet Safety Policy;
- b. Student safety with regard to:
  - i. safety on the Internet;
  - ii. appropriate behavior while on online, on social networking Web sites, and in chat rooms; and
  - iii. cyberbullying awareness and response.
- c. Compliance with the E-rate requirements of the Children's Internet Protection Act ("CIPA").

Following receipt of this training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of the District's acceptable use policies.

## **VANDALISM PROHIBITED**

Any 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. Intentional attempts to degrade or disrupt system performance will be viewed as violations of district Policies and, possibly, as criminal activity under applicable state and federal laws, including the Texas Penal Code, Computer Crimes, Chapter 33. This includes, but is not limited to, the uploading or creating of computer viruses, system break-in utilities or system hacking programs.

### **FORGERY PROHIBITED**

Forgery or attempted forgery of electronic messages, documents or files is prohibited. Attempts to read, delete, copy, or modify the electronic mail, documents or files of other system users or deliberate interference with the ability of other system users to send/receive electronic mail, documents and files 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 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 an Internet filtering software package to minimize the access to objectionable material. Any attempt to circumvent the filtering software is a violation of District policy.

A student bringing prohibited materials into the school's electronic environment will be subject to disciplinary action. An employee knowingly bringing prohibited 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 for employees.

### **Other issues applicable to acceptable use are:**

- **Copyright:** All users are expected to follow existing copyright laws
- **Supervision and permission:** A student may use a computer only if supervised and granted permission .
- **Attempting to log on or logging on to a computer or email system by using another's password is prohibited.**
- **Improper use of any computer or the network is prohibited. This includes but is not limited to the following:** •  
Submitting, publishing or displaying any defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented or bullying, threatening materials or messages, either public or private
- Attempting to or harming equipment, materials or data
- Attempting to or sending anonymous messages of any kind
- Using the network to access or post inappropriate material in public or private sites including but not limited to social media.
- Knowingly placing a computer virus or any other destructive computer code 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 authorization
- Using a network account belonging to someone else
- By-passing school proxy servers
- Posting personal information about others without proper authorization
- Downloading or using copyrighted information without permission from the copyright holder
- Attempting to "hack" into network resources
- Storing inappropriate information (i.e. jpeg and .exe files) in home directories or STU Share
- Students accessing the GISD grade book or any student data system
- Disabling or attempting to disable any Internet filtering device
- Encrypting communications to avoid security review
- Wasting school resources through the improper use of the computer system or network
- Gaining unauthorized access to restricted information or resources
- Personal printers, scanners or computers attached to the BISD network

### **SUSPENSION/REVOCAION OF SYSTEM USER ACCOUNT**

The District will reserve the right to 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 BISD Administrator provides 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 Code of Conduct or Employee Handbook.

### **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.

### **TERM**

This policy is binding for the duration of employee's employment or student's enrollment in BISD

### **ADOPTION**

This Internet Safety Policy was adopted by the Board of Bosqueville at a public meeting, following normal public notice, on June 21, 2012.

# BOSQUEVILLE ISD STUDENT AGREEMENT

Student ID: \_\_\_\_\_ Grade \_\_\_\_\_

School: \_\_\_\_\_

I understand that my computer use is not private and that the District will monitor activity on the computer system. I have read the District's electronic communications system policy and administrative regulations and agree to abide by their provisions. I understand that violation of these provisions may result in suspension or revocation of system access.

\_\_\_\_\_  
Student First Name (Please print)

\_\_\_\_\_  
Student Last Name (Please print)

Student Signature \_\_\_\_\_ Date (mm/dd/yyyy) \_\_\_\_\_

## **PARENT AGREEMENT:**

I have read the District's Guidelines for Acceptable Use of Bosqueville Independent School District Technology Resources, and this agreement form. In consideration for the privilege of my child using the District's electronic communications system, and in consideration for having access to the public networks, I hereby release the District, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my child's use of, or inability to use, the system, including, without limitation, the type of damage identified in the District's policy, and administrative regulations.

\_\_\_ I give permission for my child to participate in the District's electronic communications system and certify that the information contained on this form is correct.

\_\_\_ I do not give permission for my child to participate in the District's electronic communications system.

Parent or Guardian Name – (Please print) \_\_\_\_\_

Parent or Guardian Signature \_\_\_\_\_

Home address \_\_\_\_\_ Home phone number \_\_\_\_\_

Email address \_\_\_\_\_ Date (mm/dd/yyyy) \_\_\_\_\_

# BOSQUEVILLE ISD EMPLOYEE AGREEMENT

School \_\_\_\_\_ Position \_\_\_\_\_

I understand that my computer use is not private and that the District will monitor activity on the computer system. I have read the District’s electronic communications system policy and administrative regulations and agree to abide by their provisions. I understand that violation of these provisions may result in suspension or revocation of system access.

\_\_\_\_\_  
Name- Please Print

\_\_\_\_\_  
Signature

Date: \_\_\_\_\_