

BOAZ CITY SCHOOLS EMPLOYEE ACCEPTABLE USE POLICY
Use of Computers, Internet, and Electronic Communication Systems

I. **GENERAL**

Boaz City School System's (BCSS) employees have access to one or more forms of electronic media and services including, but not limited to, computers, email, telephone, cellular phone, voice mail, fax machines, online services, chat rooms, newsgroups, streaming media, electronic bulletin boards, Internet, and other messaging services.

The intent of this policy and supporting standards, procedures, and guidelines are to establish permitted use of these electronic media and services by BCSS employees and any other individuals granted access to these media and services.

Access to computer systems and networks impose responsibilities and obligations that are subject to BCSS policies and state and federal laws. Acceptable use of these resources involves ethical conduct, honesty, and restraint in the consumption of shared resources. Furthermore, acceptable use demonstrates respect for intellectual property; ownership of data; systems security mechanisms; and individuals' rights to privacy and freedom from intimidation, harassment and annoyance.

In general, computer users are responsible for behaving courteously, ethically, and legally. **Violations of this policy will be handled in a manner consistent with comparable situations requiring disciplinary and/or legal action.**

II. **PRIVACY NOTICE**

Access to electronic media and services described herein is provided as a tool to enhance and efficiency and effectiveness in the accomplishment of BCSS's overall goals and objectives. BCSS reserves the right to monitor, inspect, copy, review, and retain, without prior notice, information relating to usage of these electronic media and services. All materials, files, software, communications, and other content transmitted, received, or stored in connection with this usage are considered the property of BCSS. Employees and others authorized to access these electronic media and services should have no expectation of privacy regarding them. BCSS has the right to utilize records that reflect an employee's electronic media and services usage in a personnel matter. When deemed necessary, BCSS may disclose any item enumerated herein to law enforcement agencies or other third parties without consent.

**Initial: _____

III. PERSONAL RESPONSIBILITY

By accepting an account for access to BCSS's electronic media and services, each person so authorized agrees to adhere to BCSS policies regarding the use of such electronic media and services. Furthermore, each authorized person agrees to report misuse or policy violations to his/her supervisor or other designated representative at the time of receiving access to BCSS's electronic media and services.

IV. PERMITTED USE

The use of BCSS electronic media and services is a privilege, not a right. Authorized use of BCSS electronic media and services extends through an employee's term of employment or for the agreed-upon duration for others to whom such access is granted, except that access may be suspended if violations of this policy occur.

The school e-mail and Internet access may not be used for transmitting, retrieving or storage of any communications of a discriminatory or harassing nature. Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes or sexual preference shall be transmitted. No abusive, profane or offensive language is to be transmitted through the school's e-mail or Internet system. Electronic media may not be used for any other purpose that is illegal, against school policy or contrary to the school's best interest. Solicitation of non-school business or any use of the school e-mail or Internet for personal monetary gain is prohibited.

V. POLICY COMPLIANCE

Failure to comply with the Acceptable Use Policy is a serious offense and may result in suspension of access to BCSS electronic media and services described herein. Violators are also subject to disciplinary actions, including termination of employment, as deemed appropriate by BCSS. Offenders may also be subject to criminal and civil liability.

VI. APPROPRIATE USE

Each employee is responsible for the content of all text, audio or images that he/she places or sends over the school's e-mail/Internet system. No e-mail or other electronic communications may be sent which hides the identity of the sender, represents the sender as someone else or someone from another school. All

messages communicated on the school's e-mail/Internet system should contain the employee's name.

Any messages or information sent by an employee to another individual outside of the school via an electronic network (e.g., bulletin board, online service or Internet) are statements that reflect on the school. While it is customary to include personal "disclaimers" in electronic messages, there is still a connection to the school, and the statements may be tied to the school.

All communications sent by employees via the school's e-mail/Internet system must comply with this and other school policies and may not disclose any confidential or proprietary school information. Authorized users must apply good judgement at all times relative to the use of BCSS electronic media and services. The following list of requirements and restrictions is not intended to cover every possible situation but contains specific guidance regarding permitted activities and prohibited activities. BCSS reserves the right to amend and revise the list at any time.

In making appropriate use of resources, authorized users **must**:

- Only use electronic media and services for business purposes. Employees may access email and the Internet for personal use during non-working hours; however, such use will be governed by and subject to the same restrictions as described herein
- Only use legal versions of copyrighted software in compliance with vendor license requirements
- Be considerate in the use of shared resources (disk space, printer usage, network bandwidth, etc.)
- Adhere to the policies of any remote network when accessing other remote networks
- Only load software onto computers that support performance of job functions.
- Avoid any conduct through distribution or receipt of information that would be considered wasteful, offensive, obscene, illegal, or disruptive.

In making appropriate use of resources, authorized users **must not**:

- Conduct illegal activities
- Engage in political activities with the use of system resources
- Engage in any activity for personal gain or profit including the sale or solicitation of any item
- Participate in or propagate chain messages and/or executable graphics or programs
- Gamble, wager, bet, or sell chances
- Reveal or publicize proprietary or confidential information without specific authorization
- Represent personal opinions as those of BCSS

- Make or post improper remarks and/or proposals including, but not limited to, those which contain defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, discriminatory, or illegal material
- View sexually explicit material
- Make or use illegal copies of copyrighted software, store such copies on BCSS computer systems, or transmit them over BCSS networks. Violators will be personally responsible and liable for such infringing activities
- Use mail or messaging services to harass, intimidate, offend, or otherwise annoy another person
- Send electronic communication that attempts to hide or misrepresent the sender
- Engage in any activity that might be harmful to BCSS systems or information stored thereon
- Send confidential information via email unless encrypted. This would include items such as financial data, Social Security numbers, employee health records, and other personally identifiable information
- Engage in any activity that does not comply with the guidelines presented above

To prevent computer viruses from being transmitted through the school's e-mail/Internet system, there will be no unauthorized downloading. All downloaded software must be registered to Boaz City Schools. Employees wishing to download software must first contact the Information Technology Department for permission and guidance. Only authorized technicians are authorized to install software on school computers.

Employees may be issued electronic equipment for their use during and outside the traditionally school day. Employees are responsible for electronic equipment issued for their use and must immediately report loss or suspected theft of electronic equipment to Boaz City Schools administration and local police department. Employees are financially responsible for lost or stolen electronic equipment and responsible for all damages not covered by warranty or deemed acceptable as normal wear and tear. Warranties do not cover spilled liquids, damage from dropping of equipment, unprotected power surges or damaged or cracked equipment screens. Employees understand that use of this electronic equipment is a privilege, not a right and inappropriate or suspected inappropriate use will result in cancellation of this privilege, pending investigation and/or other disciplinary action.

VII. SECURITY

School and district administrators are responsible for identifying and protecting information and computer assets within their sections. The BCSS Technology department is responsible for the establishment, implementation, and maintenance of a

computer security program to assist in the protection of department assets. When appropriate, the BCSS technology coordinator shall publish standards, procedures, and guidelines necessary to assure adequate security associated with this policy.

The Electronic Communications Privacy Act of 1986 allows for schools to utilize a blocking/filtering system where it relates to review of communications once they are stored in a school or district system, monitoring for legitimate purposes where one party has previously consented to such monitoring (Acceptable Use Agreement), and monitoring by personnel performing duties necessary to maintaining the computer systems or to protecting the rights or property of Boaz City Schools. The Children's Internet Protection Act (PL 106-554) requires that schools implement technology measures to protect minors from visual depictions that are obscene, pornographic, or "harmful to minors". The staff of BCSS is subject to the provisions of the Alabama Computer Crime Act (1985).

BCSS will provide authorized users with appropriate network access instructions and information upon receipt of properly approved requests. Authorized users shall adhere to the following rules relating to network passwords:

- Passwords should be protected at all times and should not be displayed or accessible within an individual's workspace.
- Administrators may request that BCSS authorize multiple persons to have temporary access to files that may otherwise not be shared.
- Passwords should not include an individual's name, address, birthdate, username, nickname, or other identifying codes that might be easily associated with the individual.
- Sign-in procedures will require passwords to be at least eight characters long; contain a combination of letters, numerals, and special characters; and be changed automatically every 90 days.

VIII. USE/PRODUCTION OF ELECTRONIC COMMUNICATION

Every form of electronic communication can be included in the discovery process of judicial and administrative litigation, including personnel matters. This includes calendars, tasks, telephone messages relayed by electronic messaging, personal notes, and email. Electronic communication must be able to withstand public scrutiny. Therefore, authorized users must consider each electronic communication in light of it potentially being forwarded beyond the intended recipient, inadvertently accessed or disclosed, subpoenaed in a legal action, requested during the course of discovery, or otherwise made public. Accordingly, electronic communication should be drafted and

sent with at least the same level of care, professional judgement, and discretion as paper documents.

Due to the inability to guarantee the security of electronic messages, the use of electronic messages containing data of a sensitive or protected nature is discouraged. Authorized users are strongly encouraged to transmit sensitive information in other ways. Electronic messages of a confidential nature should be indicated as such in the subject line and/or in the text of the message.

Employees on the Boaz City School's e-mail/Internet system may not transmit copyrighted materials belonging to entities other than the school. All employees obtaining access to other school's or individual's materials must respect all copyrights and may not copy, retrieve, modify or forward copyrighted materials, except with permission, or as a single copy to reference only. Failure to observe copyright or license agreements may result in disciplinary action up to and including termination.

IX. USE OF ALL CALL

The general use of ALLBOAZSTAFF emails should be limited to those announcements that are of interest to at least 75 percent of all employees of BCSS. Inclusion of a subject line containing ALLBOAZSTAFF and the purpose of the message is required.

X. SOCIAL MEDIA GUIDELINES

The expectation of BCSS is that school employees will function under our district communication plan. The use of personal social media is not discouraged nor controlled by BCSS. However, it is important for employees to be reminded of best practices, since they are public employees. Once you have attached your employment status to your personal account, your posts are now connected to your school and our system. These guidelines have been established to protect each individual as an employee of BCSS, since your presence online can have an effect on your employment. Please refer to the Social Media Expectations document in your school's front office, BCSS technology department, or the Boaz City Schools' website for additional information.

Social Media Best Practices:

1. Protect your privacy online by changing your privacy settings and not friending those that you do not know.
2. All posts can be screenshot, printed, copied, and/or emailed, and locations can be easily searched.
3. Your right to free speech is protected only if you speak out as citizens on "matters of public concern," and your speech doesn't disrupt the school. Read,

- understand, and adhere to the Boaz City Schools' Acceptable Use Policy.
4. Avoid "friending" or "following" students on your personal social media accounts. Implement a rule that students can follow or friend you only after they graduate.
 5. If you want to use social media professionally, create a separate account for this and maintain appropriate boundaries and language at all times.
 6. Monitor your Internet presence. Delete any posts or comments that are questionable, and remove any pictures that are inappropriate.
 7. Avoid posting anything that places you in an unfavorable light. This includes inappropriate language, images, and posts.
 8. Avoid telling stories about work that include personally identifiable details, such as full names, job titles, addresses, phone numbers, pay, or other information protected by state and federal privacy laws.
 9. Keep all student information private.

XI. SURVEILLANCE CAMERA NOTIFICATION

BCSS monitors all school building common areas with security camera surveillance.

XII. MEMORANDUM OF UNDERSTANDING

Memorandum of Understanding for BCSS Internet Users

I, _____, am requesting to be given access to BCSS's network for use for the performance of my job. I have read the BCSS Acceptable Use Policy. I further understand that violations can result in disciplinary actions for misuse of state resources as described in the Policy.

Signature: _____

School: _____

Date: _____

A copy should be kept by the employee after signature, and the original will be filed by the employee's school and/or district administrator.