Technology Acceptable Use and Internet Policy

Buncombe County Schools (BCS) is committed to providing a safe, caring, rigorous, and engaging learning environment that prepares all students to be Career and College Ready. Accessing and using technological resources comprises one of the keystones of a 21st Century education; this document contains the policies and responsibilities necessary for the acceptable use of BCS computers, digital resources, and other personal wireless devices on BCS campuses. Using these resources responsibly will promote educational excellence by facilitating resource sharing, fostering creativity, and promoting communication in a safe, secure environment for all users.

Statement of Objective

BCS provides network, computer, and digital resources to provide educational opportunities, to promote effective instruction, to facilitate learning, and to allow for efficient communication. These objectives emphasize the primary focus of using technology for educational purposes.

As an educational organization, BCS works to ensure the safety and success of all stakeholders. Toward that end, network resources are subject to all federal and state regulations including those set forth in the national Children's Internet Protection Act (CIPA) and Neighborhood Children's Internet Protection Act (NCIPA). Some of the central requirements include the provision and use of filtered and archived email, the use of a Technology Protection Measure (TPM) to filter access to obscene or pornographic content or other content that is identified as harmful to minors, and annual certification of compliance to requirements. In addition, BCS is responsible for creating measures to protect unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Although BCS has taken precautions to restrict access to inappropriate materials, users may encounter objectionable material. However, providing access to the information and interaction available online outweighs the risk of exposure to objectionable content. BCS reserves the right to identify online content as objectionable and limit access to those resources.

I. Organizational Responsibility and Privacy

As a public school system, BCS bears the responsibility of educating, supervising, and monitoring the use of the BCS networks and digital resources.

a. Education for the safe and responsible use of digital resources is covered in North Carolina Information and Technology Essential Standards at each individual school at each level. These curricula address netiquette, password security, social networking, electronic messaging, disclosure of personal information, and unlawful online activities.

Ref: **Policy #441 Students, Student Records**
FERPA (*Family Education Rights and Privacy Act)*

c. In addition to the employment of a Technology Protection Measure, BCS staff will monitor online usage of minors and enrolled students.

d. The Technology Protection Measure may be disabled for adults, or in the case of minors, adjusted or minimized for educational purposes as recommended by members of the BCS Media and Technology Committee and approved by the BCS Director of Technology.

II. Personal Responsibilities

While BCS will educate, supervise, and monitor use of the BCS networks and digital resources, stakeholders must also be aware of and agree to the content of BCS policies and conduct themselves with safety and propriety in the digital realm.

a. Access to any BCS network constitutes an agreement to abide by BCS Board Policy 646R, "Technology Acceptable Use and Internet Policy." Access to Policy 646R is available prior to logging in, and users must agree to abide by Policy 646R or network access is denied.

b. Users must adhere to appropriate network etiquette and assume responsibilities when using any resources through the BCS network. These responsibilities warrant the following behaviors:

i. If a user identifies a security problem on the network, he or she should notify a system technology administrator or a school administrator.

ii. Users should never reveal personal information such as addresses, phone numbers, or Social Security numbers of self or others.

iii. Users should respect the Copyright of all content sent, retrieved or accessible through the Internet.

iv. Users should understand the dangers associated with Internet use: limits to security of personal data, social networking, risks of displaying photos, movies or other depictions of self, phishing emails, viruses, malware, and communications with strangers.

III. Acceptable Use

As an educational organization, BCS provides technology and Internet access to provide and promote educational pursuits consistent with the objectives of the BCS. User attitudes and activities must not interfere with the mission of providing educational content.

Ref: **Policy #441 Students, Student Records**
FERPA (*Family Education Rights and Privacy Act)*

BCS holds the following actions and attitudes as unacceptable in the BCS network environment.

a. Illegal activities are strictly forbidden. Such activities include (but are not limited to):

   i. Hacking into networks or programs

   ii. Intentionally uploading or downloading files or programs that contain computer viruses

   iii. Copying or downloading programs or files protected by Copyright

   iv. Use of a proxy in order to bypass the network filter

b. Actions that hinder access to or use of the network--tampering with equipment, vandalism, adjusting or disabling hardware or system settings, or comparable actions--are forbidden.

c. Users may not access objectionable content including but not limited to obscene or pornographic content or content that is harmful to minors.

d. Users may not use another individual's identification, log-in, or password to access or attempt in gaining access to another's account.

e. Users will not play games or use applications that are not specifically approved by an instructor or administrator.

f. No part of the network can be used for political lobbying or commercial purposes.

g. Language that is considered bullying, abusive, profane, or vulgar is prohibited.

IV. Procedures for Improper Use

While BCS bears the responsibility for the supervision of the use of the network and digital resources, the school system recognizes that the most appropriate interventions and consequences should be established and assigned on the school level.

a. Local school stakeholders will create policies and implement disciplinary actions as approved by the School Improvement Team and the school's Media and Technology Advisory Committee.

b. Local school staff and/or the BCS Technology Department will notify the Principal who will enforce the school's adopted policies.

Ref: **Policy #441 Students, Student Records**
FERPA (*Family Education Rights and Privacy Act)*

c. In cases of severe infractions, local law enforcement may be notified.

V. Personal Devices

BCS recognizes that personal electronic devices can supplement county resources and better prepare stakeholders for success in the 21st Century. However, this recognition does not preclude BCS responsibility to supervise and monitor the use of devices not owned by BCS if those devices access any part of the system's network.

a. Personal devices are not allowed on the BCSsecure wireless network or the internal network via Ethernet cable.

b. Personal devices may gain BYOD wireless access only (a segmented portion of the BCS Local Area Network).

c. BCSguest wireless Internet access is also available for visiting professionals.

d. Personally-owned wireless hotspots are not allowed for use in BCS without expressed approval of BCS Technology Department. Operations of wireless hotspots are prohibited and will be terminated immediately upon discovery and may be confiscated.

e. Disciplinary guidelines regarding the possession and times of acceptable use of personal devices connected to the BYOD network will be created at the school level by the School Improvement Team and the school's Media and Technology Advisory Committee.

VI. Web-based Resources

Although the World Wide Web is unrestricted, the range of content and applications is too broad for use in Buncombe County Schools. BCS employees and students bear the responsibility for ensuring that the use of Web-based resources adheres to the guidelines for safe and proper use established in this policy.

a. All employees are required to use approved BCS district resources when creating curricula for any and all educational and work-related postings or communications with students.

b. Employees are to maintain an appropriate relationship with students at all times. Allowing student access to a private website or private online networking profile is considered a form of direct communications with students.

Ref: **Policy #441 Students, Student Records**
FERPA (*Family Education Rights and Privacy Act)*

c. Employees are encouraged to block students from viewing any material or profiles that are not age appropriate. Any employee found to have created and/or posted inappropriate content on a website or profile that has a negative impact on the employee's ability to perform their job as it relates to working with students will be subject to discipline, up to and including dismissal. This section applies to all employees, volunteers and student teachers working for or in the Buncombe County School System.

d. Employees must conduct BCS business with students, parents, and businesses using the provided BCS email account. Conducting BCS business using a personal email account provides BCS employees no protection from any citizen to request access to the personal email account through the Freedom of Information Act.

VII. Liability Limitations and Disclosures

While BCS will always strive to provide the most efficient, safe, and appropriate resources reliably, the technological complexity of this mission makes guarantees impossible. By agreeing to Board Policy 646R, users recognize that BCS will not be held responsible in the event that service does not meet user expectations. Users also express their awareness that any information created or stored within the BCS network is not private by agreeing to board policy.

a. BCS makes no warranties of any kind, whether expressed or implied, for the services provided. BCS is not responsible for damages suffered, including the loss of data resulting from delays, non-deliveries, or service interruptions caused by its own negligence or the user's errors or omissions, or loss/damage to personal devices. Use of any information obtained via the Internet is at user's own risk. BCS specifically denies any responsibility for the accuracy or quality of information obtained through its services.

b. The inclusion of any link to a site not controlled by BCS is for convenience only and does not represent an endorsement of the site by BCS. Students, parents, and staff should be aware that connection to any Internet or network provider not under BCS control may be unfiltered. This is particularly true of open wireless connections, which are widely available and through Internet enabled smart telephone access. BCS is not responsible for unfiltered content that may be viewed or downloaded on BCS equipment that has been provided to individuals for use outside BCS network control or property. BCS will, however, remove said inappropriate content from equipment owned by BCS and will ask that, in the case of proven inappropriate content, equipment not owned by BCS be removed from school property.

Ref: **Policy #441 Students, Student Records**
FERPA (*Family Education Rights and Privacy Act)*

c. All users expressly agree that any information created or stored within the BCS network is not private. Content derived from inappropriate use of the Internet and connected resources may be provided to administration for action under Student and Personnel conduct policies of BCS. Contents within any account may be saved and provided to law enforcement as evidence for future action.

d. BCS is not responsible for personal websites or web pages created or maintained by students, personnel, parents, groups or organizations. Personal websites or web pages are not considered district-related websites or web pages.

Definitions:

USER: Anyone authorized by administration to use the BCS network. This includes, but is not limited to, staff, students, parents, vendors, contractors, and volunteers.

BCS NETWORK: All computer resources, including but not exclusive to: software, hardware, and services that allow connection of BCS computers to other computers whether they are within BCS or external to BCS.

CIPA definitions of terms:

MINOR. The term “minor” means any individual who has not attained the age of 17 years. 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:

Ref: **Policy #441 Students, Student Records**
FERPA (*Family Education Rights and Privacy Act)*

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.

Ref: **Policy #441 Students, Student Records**
FERPA (*Family Education Rights and Privacy Act)*