TECHNOLOGY ACCEPTABLE USE POLICY **Admin. Reg. OS-39 May 2023**

I. Purposes

A. This Administrative Regulation outlines the Superintendent's expectations that the Beaufort County School District (BCSD) educational networks support research and education and business activities in and among academic institutions by providing access to unique resources and the opportunity for collaborative work.

B. BCSD makes a variety of communication and information technologies available to authorized users. When properly used, these technologies promote BCSD's instructional and business purposes. Illegal, unethical, or inappropriate use may cause significant negative consequences for all users, BCSD, its students, and its employees. This document is intended to minimize the likelihood of such harm by setting standards which protect BCSD, its users, its data, and its systems.

C. The BCSD affirms the right of all individuals to be treated with respect and to be protected from intimidation, discrimination, physical harm, and/or harassment. The BCSD is committed to nondiscrimination and equal opportunity for all students, parents/legal guardians, staff, visitors, applicants for admission and employment, personnel, and community members who participate or seek to participate in its educational programs or activities. Accordingly, the BCSD does not discriminate against any individual on the basis of race, religion, gender, gender identity, sexual orientation, sex, pregnancy, childbirth, or any related medical conditions, color, physical or mental disability, age (40 or older), ancestry, genetic information, national origin, or any other applicable status protected by Title VI, Title VII, Title IX or any other local, state, or federal law.

II. Guiding Principles

A. Accessing the internet through BCSD equipment is a privilege, not a right, and inappropriate use, including violation of the Technology Acceptable Use Policy (AUP), may result in cancellation of the privilege.

B. Technology includes, but is not limited to, computer hardware, peripherals, network and communications equipment, software, web sites, mobile internet connections, and audio and video.

C. In order to maintain system integrity, BCSD reserves the right to monitor, inspect, copy, review and store, at any time and without prior notice, any and all usage of the computer network and internet access and any and all information transmitted or received in connection with such usage. All such information shall be the property of BCSD, and no user shall have any expectation of privacy regarding such materials.

D. Upon exit from BCSD, all affiliated accounts will be disabled by the administrator. The use of BCSD intellectual property and data shall be immediately discontinued and/or deleted from any and all personal devices by the exiting user. In addition, personal/individual data will not be available for restoration by BCSD upon exiting.

E. BCSD reserves the right to access/remove files, documents, devices, materials or otherwise from the BCSD network at any time and for any reason, with or without notice to any user.

F. All BCSD technology is the property of BCSD, thus all BCSD employees, students, board members and visitors are responsible for following and complying with any and all BCSD rules, administrative regulations, and procedures pertaining to technology.

G. Any person, vendor, or outside agency bringing technology into a BCSD building or connecting to or through a BCSD network shall adhere to BCSD rules, administrative regulations, and procedures.

H. BCSD technology rules, administrative regulations, and procedures shall be included in BCSD student and staff handbooks as appropriate.

I. Failure to follow BCSD rules, administrative regulations, and procedures may lead to disciplinary or other action appropriate for the infraction and for the individual. Examples include but not limited to, accounts being suspended, students being disciplined in accordance with the Student Code of Conduct, staff being referred to Human Resources for disciplinary action, removal from the approved substitute teacher list, removal from the approved volunteer list, and termination of contracts with vendors or contracted personnel. BCSD further reserves the right to notify law enforcement and/or seek criminal prosecution for violators, impose monetary penalties equal to the cost to repair or replace technology items, and/or impose any other appropriate sanction.

J. BCSD utilizes several online vendors in order to provide educational services to its students. The Children's Online Privacy Protection Act (COPPA) protects children's privacy and safety online, including restrictions on marketing to those under 13. Per COPPA guidelines, BCSD may consent on parents' behalf to a website or mobile app's collection, use, or disclosure of students' personal information, so long as that collection, use, or disclosure is solely for the benefit of BCSD, for educational purposes and not for any commercial purpose. For more information on COPPA, please visit www.ftc.gov.

K. BCSD shall comply with all state and federal statutes and regulations including, but not limited to, the Children's Internet Protection Act (CIPA), Children's Online Privacy Protection Act (COPPA) and the Family Educational Rights and Privacy Act (FERPA).

III. District Technology Resources and Usage

A. BCSD technology resources include, but are not limited to, hardware items, such as

computers, cell phones, printers, mobile devices, laptops, projectors, and interactive panels.

B. BCSD technology resources also include all software applications and tools available for use at any location in the Beaufort County School System.

C. Users of BCSD technology resources shall abide by all conditions pertaining to software license agreements and copyright laws.

D. Unauthorized use of BCSD computers and hardware items is not permitted.

E. Vandalism, unauthorized access, "hacking," or tampering with hardware or software, including introducing "viruses" or pirated software, is strictly prohibited.

F. Using resources for commercial, religious, or political activities is prohibited.

G. Using obscene, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or gang-related language or symbols is prohibited. Engaging in personal attacks against another BCSD staff or student including prejudicial or discriminatory remarks and/or threatening or harassing another BCSD staff or student using any language in an email or social media platform are also prohibited.

H. Using the district system to access, receive, distribute, or store material that is profane or obscene, pornographic, or sexually explicit; which advocates illegal acts; or that advocates violence or discrimination toward other people (e.g., hate literature), including access through the system and all network peripherals including printers, hard drives, removable disc drives, and electronic storage devices, is strictly prohibited.

I. Access of personal information or confidential BCSD information that becomes available to a computer user must be treated as privileged information. Copying, modifying, disseminating, or using this information is prohibited and subjects the offender to disciplinary action. Students will be disciplined according to the Student Code of Conduct. Staff will be referred to Human Resources for disciplinary action up to and including dismissal per Human Resources guidelines. For any persons, criminal prosecution may be initiated.

J. No user shall willfully or deliberately damage or unlawfully remove BCSD technology, network resources, or BCSD data.

K. Any willful act or omission that could cause either general loss of service or data, or interference with the work of another user, shall be cause for disciplinary action.

L. In the event a person loses or causes damage to BCSD computer files, hardware, software, or other computer related equipment, BCSD may seek from such person full restitution for the actual replacement cost to the BCSD, including but not limited to labor, parts, materials, and related costs.

M. Protection and backup of data on a district issued device is the student or staff member's sole responsibility. BCSD shall not be liable for loss of data. If a device must be re-imaged due to a malfunction or repair, data stored on the device could be lost. BCSD offers cloud storage and network storage space which gets backed up nightly.

IV. Software/Hardware Management

A. Purchases of technology resources shall be made in accordance with BCSD Admin. Reg. IS-37. Procurement of technology resources other than through the procedure contained in Admin. Reg. IS-37 is prohibited and will be considered unauthorized.

B. BCSD shall maintain a list of application software and programs approved for use on the BCSD computers.

C. No software or programs shall be installed on BCSD computers or servers without the proper license or permission.

D. Only software and programs purchased, owned, or explicitly authorized by BCSD shall be installed on BCSD computers. No personal software may be installed and used without prior authorization from the BCSD Technology Department. This includes, but is not limited to, games, productivity software, utilities, and communication software.

E. Copying and/or duplication of BCSD software and/or programs for any reason is prohibited.

F. BCSD will re-image a device or remove any non-approved software or applications discovered on BCSD computers or networks. Removed software and/or applications will not be returned to the installing user or the person to whom the BCSD device was issued. Students will be disciplined according to the Student Code of Conduct. Staff will be referred to Human Resources for disciplinary action up to dismissal pursuant to Human Resources guidelines.

G. BCSD approved and purchased systems/software that are no longer in compliance with current security patches and policies will be removed/discontinued at the discretion of the BCSD Technology Services Officer. All systems that require service contracts to maintain compliance shall be purchased by the original budgeting department until such systems are no longer in use. If the system creates a significant strain on technology resources, the purchasing department and/or school may be required to purchase hardware in order to support the requested system/software.

H. Only BCSD approved and purchased systems/software shall be supported by BCSD technology staff.

V. District E-Mail

A. Email by and through district email accounts is a business communications tool. Users must use this tool in a responsible, lawful manner. Only BCSD business should be conducted on BCSD email.

B. Students are provided a Google (beaufortschools.org) email address when enrolled with BCSD. To protect students from spam and inappropriate contact with non-BCSD individuals, these email accounts are closed to only internal BCSD communications and required software vendor domains.

C. Under certain circumstances, email may be considered public records under the S.C. Freedom of Information Act (FOIA) and therefore subject to disclosure upon proper request, unless exempt from disclosure under one of the exemptions provided in the FOIA.

D. Under certain circumstances, email also may be considered student education records under the Family Educational Rights and Privacy Act (FERPA), subject to the rights of parents/legal guardians and eligible students, and with limited exceptions others, to inspect and review.

E. Any mass email sent to over 100 users must first be approved by Chief Human Resources Officer or the Director of Communications. Any attempt to circumvent this policy may lead to disciplinary measures against the BCSD employee.

F. It is strictly prohibited to:
   i. Send or forward emails containing libelous, defamatory, offensive, racist, or obscene remarks.
   ii. Sending or forwarding a message with sensitive information, including credit card numbers, bank account numbers, routing numbers, driver's license numbers, social security numbers, or any protected information. For security reasons, credit card numbers, bank account numbers, routing numbers, driver's license numbers, and social security numbers are blocked from being emailed by the Administrator.

VI. Technology Network

A. The BCSD Technology Services Officer or his/her designee will provide all BCSD staff, students, board members, contractors and other approved entities with an access account to the BCSD network.

B. It is the sole responsibility of a user to ensure passwords are unique and difficult to guess by another individual. In addition, users shall safeguard their credentials from all other persons. Any and all activity on the BCSD network conducted under a set of credentials is the responsibility of the owner of said credentials.

C. Users on the BCSD network may access only those files for which they have specific

authorization.

D. The BCSD Technology Services Officer will set quotas for disk usage space for all users on the BCSD network.

E. BCSD students/staff/other entities covered by this policy shall not attempt to bypass or interfere with security systems and/or content filters on the BCSD network or with BCSD owned devices.

    a. As a baseline, student filtering is centered on categories designated by the Children's Internet Protection Act (CIPA). BCSD has added additional categories to block in an effort to better tune the device to its intended educational purpose.
    b. Over half a million websites are created every day and countless sites are edited or altered. A site which had acceptable content one day may have inappropriate content the next. As a result, content filtering is an ever-evolving system. If a student gains access to a proxy site or other inappropriate content not caught by the filtering group, it is imperative staff members notify the Technology Department immediately so those sites can be manually blocked.

F. Only devices which are owned, managed, and controlled by BCSD are authorized to be on "internal" BCSD networks.

G. In order to ensure adequate bandwidth is available for instruction and maintain a high level of network security, the Guest network is provided for the express purpose of internet access for presenters and hired contractors at BCSD facilities. It is not for staff access and under no circumstances shall it be used for student access.

H. All copyright laws (see AR OS-38) shall be followed. Making or distributing copies of copyrighted material that includes text, pictures, video, and digital media without authorization is prohibited. Only commercial or institutional based audio/video streaming services may be considered for use and must comply with all BCSD Technology Services requirements. Said services must first be vetted and approved by BCSD Technology Services for use. The use of any other subscription-based video/audio streaming service is not allowed as these services are not authorized for commercial or institutional settings and will violate the terms of service.

I. The use of the BCSD network to obtain, distribute, or store inappropriate materials is prohibited.

VII. Incidental Personal Use

As a convenience to our users, incidental use of the district's network systems is permitted. The following restrictions apply:

A. Incidental personal use of internet access or district issued devices is restricted to approved users of the information systems. It does not extend to family members or other acquaintances.

B. Incidental use must not result in direct costs to BCSD.

C. Incidental use must not be used for personal monetary gain.

D. Incidental use must not interfere with an employee's work duties or impact district network performance.

E. No files or documents may be sent or received which could result in legal liability against or embarrassment to BCSD.

F. BCSD assumes no liability for loss of an employee's personal files or documents stored on the district's networks or other digital resources, whether those personal files or documents are lost through accident, system failures, or intentional removal.

VIII. Data & Records Retention

A. BCSD recognizes the importance of maintaining complete and accurate records in compliance with all applicable law and regulations.

B. BCSD will establish and maintain a system for the securing, cataloging, and storing of all records in compliance with state and federal law. Such system will include the suspension of routine record destruction practices, as applicable.

C. The Superintendent or his/her designee will establish procedures in compliance with the South Carolina Public Records Act, the State FOIA, and/or the electronic records management guidelines established and recommended by the South Carolina Division of Archives and Records Management.

D. BCSD records management manual, incorporated in Administrative Rule OS-40, describes BCSD procedures for the retention of BCSD data and records. Any additional and appropriate forms and guidelines that support this administrative regulation are published as separate documents. Copies of the BCSD administrative rules, forms, and guidelines will be available online, at each school and the district office.

E. In the event that any state and/or federal statutes, regulations, and/or policies conflict with BCSD records retention guidelines, the state and/or federal statutes, regulations, and policies will supersede and take precedent over BCSD guidelines.

Adopted: March, 2016

Revised: February, 2021; May 2023

NOTE: IS-40 (Acceptable Use Policy), IS-40 R(1) (Internet Safety) and IS-40 R(2) (Network and Internet Acceptable Use) were replaced and incorporated into Administrative Regulation (OS-39) with the December, 2020 revision.

Legal references:

A. S. C. Code, 1976, as amended:
   1. Section 30-4-10, et seq. - South Carolina Freedom of Information Act.
   2. Sections 30-1-10 through 30-1-140 - Public Records Act.
   3. Sections 26-6-10 through 26-6-210 - South Carolina Uniform Electronic Transactions Act.

B. South Carolina Department of Archives and History Regulations 12-901 through 12-906.6 - Article 9 - General retention schedules for school districts.

C. South Carolina Department of Archives and History - Electronic Records Management Guidelines (E-Mail Management).

D. Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. 6501–6505.

E. The Family Educational Rights and Privacy Act (FERPA) 20 U.S.C. § 1232g; 34 CFR Part 99.

F. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Pub.L. 104-191, August 21, 1996, 110 Stat. 1936.

G. The Children's Internet Protection Act (CIPA) Pub.L. 106–554, Dec 21, 2000, 114 Stat. 2763, 2763 A-335, 20 USCA § 7001.

H. Beaufort County Schools Coherent Governance Manual:

   1. GC-1 Board Purpose.
   2. GC-2 Governing Commitments (GC 2.1, 2.2, 2.3).
   3. GC-3 Board Job Description (GC-3.4.b.c.d., 3.17).
   4. GC-6 Annual Work Plan.
   5. GC-11 Diversity Statement and Goals.
   6. B/SR-4 Authority of the Superintendent.
   7. B/SR-5.8 Superintendent Accountability.
   8. OE-1 Global Operational Expectation.
   9. OE-3 Treatment of Stakeholders (OE-3.1, 3.3).
   10. OE-4 Personnel Administration.
   11. OE-10 Communicating with the Board (OE-10.1, 10.2, 10.4, 10.6, 10.12, 10.16).
   12. OE-11 Communicating with the Public (OE-11.1, 11.2.a.b.c).
   13. OE-16 FOIA (OE-16.1, 16.2).