Technology Use Guidelines by Adults for 2023-2024

Purpose

To establish clear guidelines for all employees, staff members, and guests who may have or are granted access to the Bedford County Public Schools' ("BCPS") computer system.

Definitions

"Computer system" includes, but is not limited to hardware, software, data, communication lines and devices; printers; laptop and desktop computers; tablets; smartphones; optical disks; tape drives; servers; mainframe; personal electronic devices brought as part of the *Bring Your Own Device ("BYOD")* program; all peripherals, digital cameras, document cameras, interactive whiteboards/panels, and projectors; internal and external network connections; email systems; social media accounts; cloud or other online services offered through or operated by BCPS; and any other internal or external networks and/or services that BCPS utilizes.

"Division personnel," "employee," or "staff" means any person employed by the Bedford County School Board.

"Guest" means any member of the Bedford County community or other individual who is granted access to BCPS' computer system.

"Parent" means biological parent, relative, guardian, or other adult who has physical and/or legal control and responsibility for a minor (child) under the age of eighteen years.

"Student" means any person currently enrolled in Bedford County Public Schools. This includes students who are otherwise adults enrolled in any program sponsored by Bedford County Public Schools.

"User" means any person who has access to or has permission to use BCPS' computer system. User includes all guests, division personnel, employees, staff, parents, and students.

Statement of Expectations

All uses of BCPS' computer system shall be consistent with the School Board's mission: Bedford County Public Schools will provide equal opportunities to enable all students to think critically, collaborate, create, communicate, and become productive citizens. BCPS' computer system is maintained for the mutual benefit of all users, and adherence to this Technology Use Guidelines ("TUG") is necessary for continued access to the computer system.

The use of BCPS' computer system is a privilege, not a right, and the TUG and Acceptable Computer System Use (AUP) policy are designed to establish clear guidelines for all users who have been granted access to the computer system. All uses of BCPS' computer system shall be in furtherance of BCPS educational objectives and shall be in accordance with this TUG, the Code of Student Conduct, AUP and any other policy and/or procedure referenced below.

Rights and Responsibilities

Division Personnel: All division personnel shall abide by this TUG and shall not share their passwords or specific account information with any student.

Additional guidelines for acceptable electronics use are located in the School Faculty Handbooks which shall be followed by all division personnel. It is the responsibility of every user who identifies a security issue or problem to notify immediately the building administration, the Technology Staff, the Systems Engineer, or the Director of Technology.

Instructional personnel are further responsible for the following:

- To embed the use of technology as a tool to personalize learning for all learners as appropriate;
- To monitor and manage the student use of the computer system in order to protect their safety and security;
- To monitor and supervise learning activities that include the integration of technology;
- To educate and support students in Internet safety, the Fair Use Act, and copyright law;
- To ensure that all guests receive a copy of this Policy before they may access the computer system;
- To participate in professional development opportunities designed to further the understanding of technological integration in the classroom and/or to further the understanding of 21st Century Skills in the classroom;
- To participate in community outreach programs as required to educate and instruct students, parents, and community members about the dangers and pitfalls associated with improper Internet use;
- To ensure that all security measures are adhered to for the protection of all students and the BCPS computer system;
- To ensure bandwidth resources are not used in an exorbitant manner for long periods of time (e.g., unnecessary use of bandwidth-intensive sites such as audio and video streaming services), especially during test administration windows;
- To log off the BCPS network when equipment will be left unattended for extended periods of time; and
- To back up his or her individual files and documents each week.

Parents: All parents are responsible for reading this TUG and AUP in their entirety prior to signing it. Parents shall be responsible for explaining the contents of the TUG and AUP to their child(ren). Any parent granted user status to BCPS' computer system is responsible for the following:

- To follow this TUG and the AUP;
- To use BCPS' computer system for purposes consistent with the educational objectives of BCPS; and
- To notify the building administration, the Technology Staff, the Systems Engineer, or the Director of Technology immediately upon identifying a security issue or problem with the computer system.

Guests: All guests who are granted user status to BCPS' computer system shall be responsible for the following:

- To read this TUG and the AUP prior to the initial use of the computer system;
- To follow this TUG and the AUP;
- To use the BCPS computer system for purposes consistent with the educational objectives of BCPS; and
- To notify the building administration, the Technology Staff, the Systems Engineer, or the Director of Technology immediately upon identifying a security issue or problem with the computer system.

Internet Safety Instruction and Community Outreach

The need for Internet safety instruction and community outreach programs is assessed by building administrators, teachers, and other division personnel, all working together toward educating all stakeholders within our community.

As set forth in Va. Code § 22.1-70.2, BCPS shall provide to all students (K-12) Internet safety training. All students are expected to actively practice proper network etiquette. Internet safety instruction and community outreach shall be conducted periodically to educate and instruct students and parents about the dangers and pitfalls associated with improper Internet use. This includes, but is not limited to, intellectual property rights, online predators, illegal downloading from the Internet, and "sexting." Internet safety instruction and community outreach programs may call on School Resource Officers to assist in the explanation of the following: legal definitions, charges that may be filed against an individual in specific situations, and lasting legal consequences.

Safety Measures and Limitations

Software is installed on the BCPS network to filter or block any content deemed inappropriate or harmful by BCPS, which includes but is not limited to child pornography as set out in Va. Code § 18.2-374.1:1 or as defined in 18 U.S.C. § 2256; obscenity as defined in Va. Code § 18.2-372 or 18 U.S.C. § 1460; material that the school division deems to be harmful to juveniles as defined in Va. Code § 18.2-390, material that is harmful to minors as defined in 47 U.S.C. § 254(h)(7)(G), and material that is otherwise inappropriate for minors including social networking spaces. Software filters are limited to blocking content accessed through the BCPS' network, and will not prevent access to content when non-BCPS networks are utilized. Cell phones are one example of technology that do not utilize the BCPS network and will not benefit from the software filter. Users shall not rely on software filters to prevent inappropriate website access. Concerning the use of Voice over Internet Protocol (VoIP) phones, calls may be monitored or recorded for record-keeping purposes.

As new technologies emerge, the educational value and ease of classroom integration will be evaluated concurrently by the BCPS Technology Staff, the BCPS Instructional Department, the BCPS Special Services Department, building technology committees, and the TUG Committee. Recommendations for amendment to the TUG and AUP will be made by the TUG Committee to the School Board.

Data Backup and Network Security

BCPS makes every effort to provide reliable storage for all programs and files on BCPS' devices and through Google Drive; however, since no storage solution is 100% reliable, each user is responsible for backing up their individual files.

Users shall not expect any data stored on the BCPS' computer system to be private. Digital communication and files stored on BCPS' computer system are regarded as property of BCPS. Authorized administrators may, without reason or prior notice, review files and documents including, but not limited to, email, documents, and logs, to ensure users are acting in accordance with this TUG, and to maintain system integrity.

Current security measures include firewalls, Internet filters, virus protection, and virus monitoring devices. The BCPS Technology Staff and Systems Engineer evaluate the security of the BCPS' computer system to identify security threats daily. Data security and network security are constantly reviewed and, when necessary, adjustments and modifications are made to the system as issues arise.

Any user who identifies a security issue or problem shall immediately notify the building administration, the Technology Staff, Systems Engineer, or the Director of Technology. The intentional destruction or vandalism of BCPS' computer system by any means or the intentional breach of BCPS' LAN or WAN is prohibited. This includes, but is not limited to the use of cellular hotspots, personal access points, VPN, and/or proxy applications to circumvent the BCPS Internet filtering system. Any violation of this TUG shall result in loss of computer system privileges and may also result in appropriate disciplinary action, as determined by the School Board, or legal action.

Reliability of the Computer System

Technology, while extremely valuable, is sometimes unreliable. The School Board makes no warranties for the computer system it provides. The School Board shall not be liable for any damages to the user from use of BCPS' computer system, including loss of data, non-delivery or missed delivery of information, or service interruptions. The School Board denies any responsibility for the accuracy or quality of information obtained through BCPS' computer system. Users are cautioned to prepare for and guard against instances of technology unreliability. Users agree to indemnify the School Board for any losses, costs, or damages incurred by the School Board relating to or arising out of any violation of this TUG.

Care for Devices

BCPS staff issued a device are responsible for the general care of that device and charger assigned to them. Devices that are broken or fail to work properly must be reported to the school IT Technician. The cost to repair damage to a BCPS issued device resulting from neglect will be the responsibility of the staff member. General care and precautions:

- Only use a clean, soft cloth to clean the screen, no cleansers of any type.
- Cords and cables must be inserted carefully into the device to prevent damage.
- Devices must remain free of any writing, drawing, stickers, or labels that are not the property of Bedford County Public Schools.
- Devices are very sensitive to extreme heat and extreme cold. Therefore leaving them in cars, direct sunlight, etc. that may expose them to these conditions is potentially harmful to the device and should be avoided.
- Do not stack any books, heavy materials, etc. on top of the device as it could cause it to break.

Note: Devices MUST remain at base schools for teachers that are out for extended leave or absence unless appropriate authorization is given by the building administrator.

Google Domain

The BCPS Google Domain, a private BCPS learning management tool, is a set of intelligent apps including Gmail, Docs, Drive, Calendar and Classroom designed to promote critical thinking, creativity, collaboration and communication between students and teachers in an instructional setting.

BCPS may provide a Google Domain account to staff as a tool to meet education expectations while fulfilling academic and school-sponsored activities. A Google Domain account is not private and may be monitored and accessed by BCPS. Unauthorized access to a Google Domain account is prohibited. Users are prohibited from sharing their Google account access information (logins and passwords) with other users. Users are prohibited from soliciting or using the account access information of others. Users shall be held personally responsible for all content in their Google Domain accounts stored in Gmail, Docs, Drive, etc. When communicating with BCPS staff through Gmail, students shall use the BCPS staff member's official email address. Downloading any file attached to an electronic message is prohibited unless the user is certain of that message authenticity and the nature of the file.

YouTube is offered to staff and students through the Google Domain. A limited number of videos appropriate for school use are available in a Restricted Mode. Videos that are not available but have an educational purpose may be approved through BCPS teachers and staff. Application should only be used for educational purposes tied to staff and student's current course content and needs.

Electronic Mail (Email)

BCPS provides email to aid staff in fulfilling their duties and as an educational tool. Email is not private and may be monitored and accessed by BCPS staff. Any correspondence disseminated through the BCPS email system is considered official business and property of BCPS. Users shall be held personally liable for the content of any email they create. It may also be considered public information depending on its content. Therefore, all electronic messages sent from a BCPS email account will be uniform and consistent in the identification of the authors and/or senders. Email signature blocks will be limited to the following: first name, last name, job title, school/location, email, school phone number and have the option to use the Bedford County Public School logo.

Example:

John A. Smith, Ed.D.
English Teacher
Liberty High School
john.smith@bedford.k12.va.us
540-586-2541

Personal email accounts shall not be utilized by any BCPS staff when communicating with students or other stakeholders as a representative of BCPS. Unauthorized access to an email account by any user is prohibited. Downloading any file attached to an email is prohibited unless the user is certain of its authenticity and the nature of the file. Prohibited uses of BCPS provided email accounts included but are not limited to:

- Sending personal and confidential student information (staff shall not include confidential student information);

- Swearing, using vulgarities, or using any other inappropriate language in any email transmission (Disciplinary action, as outlined in this TUG and the AUP, may be imposed);
- Failing to check email inbox on a regular basis;
- Sending or forwarding chain letters;
- Spamming (sending unwanted, unsolicited emails to large groups of people, or everyone in your address book);
- Sending or sharing documents with large groups of people for anything other than an educational purpose to include selling products or offering outside merchandise;
- Subscribing to mail or notification lists (e.g. signing up or creating accounts for anything not school related);
- Sending emails with false or defamatory information; and
- Sending emails that are intended to harass, insult, or are personal or discriminatory attacks on another user.

Electronic & Digital Published Media

BCPS may provide digital tools to aid students and staff in fulfilling their educational and workplace responsibilities. When authoring these digital works, users shall keep in mind that the end product shall support the educational objectives of BCPS. Every member of the BCPS community has the responsibility to maintain and enhance BCPS' public image and to use all digital tools in a productive manner. Unacceptable use includes but is not limited to:

- Posting personal and/or confidential information;
- Swearing, using vulgarities, or using any language inappropriate for a school setting;
- Transmitting false or defamatory information;
- Creating any end product intended to harass, insult, or launch a personal or discriminatory attack on an individual or group; and
- Posting electronic media for any other purpose that is illegal, against School Board Policies, or contrary to the best interest of BCPS.

Social Media

Social media includes Internet-based applications and mobile technologies that allow the creation and exchange of user-generated content. Examples of commonly used social media tools include, but are not limited to blogs, message boards, chat groups, instant messaging, personal news updates, and music/video sharing (e.g., Facebook, Instagram, Remind, YouTube, and Twitter). Utilization of social media on BCPS' computer system is permitted only by division personnel for professional development purposes; as a tool to foster closer community/school relations (e.g. the creation of a school Facebook Page); and as an educational tool with students over the age of 13 years, provided it is on the pre-approved list maintained by the Director of Technology or designee.

Any use of social media must be in conformance with this TUG. Staff and students are cautioned that even non-school division computer system use of social media that violates this TUG, any School Board policies or procedures, the Code of Student Conduct, or creates a foreseeable risk of causing a substantial disruption to the work and discipline of the school may result in disciplinary action.

BCPS staff utilizing social media as a means to communicate with students and families must maintain a professional social media platform. Staff should only interact with students through social media sites

created for educational purposes. <u>Staff should not engage students through personal social media sites</u>. **Professional vs. Personal Social Media**. Professional social media is work-related and used to connect with the school community. Professional accounts and sites should be set up with a professional email address. Personal social media is non-work related. For example, staff might use a personal social media platform to connect with friends and family. Personal social media accounts and sites should be set up with personal email addresses.

Social media in the classroom shall be used with students under the age of 13 years <u>only</u> where allowed by law (e.g., falls within the parameters of COPPA, CIPA, and PPRA) or when BCPS has approved usage division-wide (e.g., the BCPS Google Domain, a private BCPS learning management system).

Examples of Acceptable Technology Use

1. Professional Development Activities
2. Comply with fair-use laws and copyright regulations while accessing the Internet
   - Understand, recognize, and respect the intellectual property of others;
   - Present accurate information when collaboratively gathering or sharing information (e.g. avoid Wiki vandalism);
   - Ethical gathering and/or presentation of information (e.g. avoid plagiarism, provide correct attribution, follow Creative Commons Law); and
   - Cite all sources.
3. School-sponsored emails
   - Used for legitimate BCPS academic and curricular activities communications;
   - Keep passwords and logins confidential;
   - Only access your own account;
   - Send messages that contain content in accordance with this TUG and the AUP;
   - Immediately report messages that violate this TUG, AUP, or the Code of Student Conduct to administration; and
   - Download attachments only when the user is certain the attachment is safe for the Computer System.
4. The Principles of the Computer System Community
   - Exercise polite and proper network etiquette (the acceptable behavior the Internet community expects its citizens to follow);
   - Use the BCPS network for educational activities – information posted to BCPS sponsored sites must be limited to curriculum related material;
   - Respect both your own privacy and the privacy of others; and
   - Respect the rights of others by not wasting network resources.

Examples of Unacceptable Use

Users MAY NOT engage in any conduct that violates this TUG or the AUP. For example:

1. Circumventing or attempting to circumvent the BCPS' filtering software
2. Swearing, using vulgarities, or any other use of inappropriate language in any electronic communication
3. Accessing web pages or Internet content that is inconsistent with the educational objectives of BCPS

4. Participating in cyberbullying which is defined as the use of electronic media to support deliberate, repeated, and hostile behavior by an individual or group with the intention of physically or psychologically intimidate others
5. Allowing students to use BCPS assigned teacher devices especially while signed in with their staff account furthermore teachers should not allow other staff to use their BCPS assigned device while they are signed in with their staff account and should never give another staff member their user account information
6. Using the network/Internet for any illegal activity, including violation of copyright law, violation of contracts, or transmitting any material in violation of any federal, state or local law
7. Sending, receiving, viewing, or downloading illegal or otherwise prohibited material via BCPS' computer system
8. Installing or downloading media, without authorization, to any BCPS or non-BCPS electronic devices while connected to the BCPS network
9. Using BPCS' computer system for private financial or commercial gain or advertising.
10. Using resources wastefully (e.g. bandwidth, file space, paper, and ink/toner) or failing to respect the BCPS resource limits
11. Gaining unauthorized access to resources or entities
12. Using BCPS' computer system after access privileges have been suspended or revoked
13. Vandalizing BCPS' computer system, including, but not limited to, modifying or rearranging keyboards, individual keycaps, any other peripheral equipment, or destroying data by creating or spreading viruses and/or by any other means
14. Forging, intercepting, or interfering with emails messages
15. Using BCPS' computer system to disrupt others
16. Snooping, phishing, keylogging, monitoring or any other known hacking tool and/or resources
17. Violating any School Board policy or regulation while using BCPS' computer system

Possible Consequences for Violating this TUG

Any division personnel who violate the TUG and the AUP shall be subjected to disciplinary action up to and including termination. Examples of possible dispositions (in no particular order) include but are not limited to:

- Supervisory conference
- Letter of reprimand
- Restriction or cancellation of technology privileges
- Restitution
- Plan of improvement
- Administrative leave pending a hearing
- Confiscation
- Law enforcement agency involvement
- Termination of employment

TUG Review and Revision

At a minimum, this TUG will be reviewed on an annual basis. Additional review may be conducted if warranted under the circumstances.