BOE Faculty/Staff Technology Policies

Technology is an ever-changing part of all of our lives and an integral part of education. Expanding technologies take students and staff beyond the confines of the classroom and provide tremendous opportunities for enhancing, extending, and rethinking the learning process. Bedford County Schools (BCS) is committed to preparing students to live responsibly in a digital world. The computing resources at BCS support educational, instructional, researching, and administrative activities. As a user of these resources, faculty and staff must behave in a responsible, ethical, and legal manner. This document serves as the Technology Policies for governing the usage of technology for all BCS teachers and staff.

BCS faculty and staff should respect the rights of other computer users and the integrity of technology resources along with all pertinent license agreements. If an individual is found to be in violation of the stated technology policies, BCS will take necessary action. Technology policies apply to all users of computing and networking resources (hardware or software) owned or managed by BCS.

General Technology Polices

With access to computers and people all over the world comes the potential availability of material that may not be considered to be of educational value in the context of the school setting or that may be harmful or disruptive. Because information on networks is transitory and diverse, BCS cannot completely predict or control what users may or may not locate. BCS believes that the educational value of limited access to the information, interaction, and research capabilities that technology offers outweighs the possibility that users may obtain or encounter material that is not consistent with the educational goals of BCS.

In accordance with the Children's Internet Protection Act (CIPA) by the Federal Communications Commission, BCS operates and subscribes to filtering software to limit users' Internet access to materials that are obscene, pornographic, harmful to children, or otherwise inappropriate, or disruptive to the educational process, notwithstanding that such software may in certain cases block access to other materials as well. At the same time, BCS cannot guarantee that filtering software will in all instances successfully block access to materials deemed harmful, indecent, offensive, pornographic, or otherwise inappropriate. The use of filtering software does not negate or otherwise affect the obligations of users to abide by the terms of this policy and to refrain from accessing inappropriate materials.

No technology is guaranteed to be error-free or totally dependable, nor is it safe when used irresponsibly. Among other matters, BCS is not liable or responsible for

- Any information that may be lost, damaged, or unavailable due to technical, or other difficulties
- The accuracy or suitability of any information that is retrieved through technology
- Breaches of confidentiality
- Defamatory materials
- Consequences that may come from failure to follow BCS policy and procedures governing the use of technology

Faculty and staff are to act ethically, respectfully, academically honestly, and supportively of student learning. All users have the responsibility to respect others in the school community and on the Internet. Users are expected to abide by the generally accepted rules of network etiquette.

Cyberbullying will not be tolerated and will result in severe action.

No user of technological resources, including a person sending or receiving electronic communications, may engage in creating, intentionally viewing, accessing, downloading, storing, printing, or transmitting images, graphics (including still or moving pictures), sound files, text files, documents, messages, or other material that is obscene, defamatory, profane, pornographic, harassing, abusive, or considered to be harmful to minors.

The following actions are not permitted while using the school network, technology equipment, BCS managed software/accounts, or Internet access:

- Send, display, or download offensive communication or media.
- Use obscene language.
- Harass, insult, attack, or defame others.
- Intentionally damage school technology equipment or network infrastructure.
- Attempt to enter network areas not related to specific classroom.
- Violate copyright laws.
- Use other users' passwords or identifiers without authorization.
- Trespass in other users' files, folders, or work.
- Intentionally misuse resources.
- Install or download software unless directed to do so by a teacher.
- Illegally duplicate software, music, or video media.
- Attempt to bypass system protection including the creation or use of proxy servers or websites.
- Use the network for commercial use.
- Reveal personal address or phone numbers nor those of students or fellow school personnel.
- Intentionally introduce a virus or malware to technology equipment or network.
- Access and use social networking or media for non-educational purposes.
- Perform any action which violates existing Board Policy or Public Law.
- Stream audio or video for anything other than educational use.
- Send electronic communications fraudulently (i.e., by misrepresenting the identity of the sender).
- Engage in hacking of any kind, including, but not limited to, the illegal or unauthorized access.

Microsoft 365 Accounts

BCS will provide Microsoft 365 accounts to all teachers and certain staff members. These accounts provide access to Microsoft's online suite of Office applications, online storage, email, and many other products. These accounts will be utilized to support educational and administrative activities. The use of these services must be consistent with BCS's educational goals and comply with local, state, and federal laws and BCS policies.

Users are advised that electronic data and communications using the BCS Microsoft 365 account and/or email address may be reviewed and/or accessed. Users should not expect that email or file storage on BCS accounts will be private. BCS reserves the right to log, monitor, and examine digital communications and content. Users must recognize that there is no assurance of confidentiality with respect to access to transmissions and files by persons outside or persons inside BCS. Also, faculty and staff email are archived for a set number of years.

Email users have a responsibility to learn and comply with BCS's policies for both system and personal devices.

The following actions are not permitted

- Share user credentials (username/password) to another user.
- Intentional and unauthorized access to other people's email or MS 365 account.
- Sending "spam," chain letters, or any other type of unauthorized widespread distribution of unsolicited mail.
- Use of email for commercial activities or personal gain (except as specifically authorized by BCS policy and procedures).
- Use of email for partisan political or lobbying activities.
- Use of email for personal social media accounts.
- Sending of messages that constitute violations to BCS's policies.
- Creation and use of a false or alias email address in order to impersonate another or send fraudulent communications.
- Use of email to transmit materials in a manner which violates copyright laws.
- Solicit or distribute information with the intent to incite violence, cause personal harm, damage a person's character, or to harass another individual.
- Respond to messages that are suggestive, obscene, belligerent, or threatening or make another user feel uncomfortable. If a user receives such a message, he or she should provide a copy of the message to administration immediately.

BCS faculty and staff should be careful not to open unexpected attachments from unknown or known senders nor follow web links within an email message unless the user is certain that the link is legitimate. Following a link in an email message executes code that can also install malicious programs on the workstation.

BCS Microsoft 365 passwords are managed by the BCS Technology Department. If a user is concerned that his or her password has been compromised, he or she must notify technology liaison immediately. Compromised passwords will be changed upon request.

BCS attempts to provide secure, private, and reliable email and Microsoft 365 services by following sound information technology practices. However, BCS cannot guarantee the security, privacy, or reliability of said services. All users, therefore, should exercise extreme caution in using BCS email to communicate confidential or sensitive matters. Also BCS email accounts are part of Microsoft's online 365 platform and utilizes Microsoft's email filtering system for protection as well as a third-party filtering system. However, good email practices are the best protection.

Staff Personal Wireless Access

The Bedford County School System provisionally offers a staff personal wireless network for educational purposes only. It will provide the same filtered Internet service that school computers currently use. The staff wireless network is for certain school system staff only. It is not available for outside users. This network offering is a privilege which the system grants to faculty and staff willing to assume the responsibility of abiding by the guidelines set forth in this document. All policies set in place in the General Technology Policy continue to apply when the employee uses his/her personal technology device on school property.

When attached to the BOE-Staff network, personal technology devices brought on school property and used during the school day are subject to search by administration if misuse is suspected. The Bedford County Department of Education (BOE) does not guarantee the privacy or security of any item stored on or transmitted by any personal technology device. The BOE Technology Department reserves the right to review Internet usage and access data files, email, and other communications utilizing the BOE-Staff wireless network. BOE takes no responsibility for any issues that result from access the BOE-Staff network.

Items that are considered personal technology devices (PTD) include but not limited to:

- Laptops
- Netbooks / Chromebooks
- iPad / iPods
- Smartphones
- Tablets
- Kindles / Nook / or other similar device

Items that are not allowed on any BOE wireless network:

- Video streaming devices such as an AppleTV, Roku, or Chromecast
- Wireless-connected printers

Guidelines:

- Administration and Technology Staff have the right to refuse to allow personal technology devices on the network and/or revoke network access.
- The BOE assumes no responsibility or financial liability for any damage the employee may incur, including but not limited to theft, physical damage, and loss of data or software malfunctions of personal technology device.
- PTDs cannot be used for media streaming, social networking, video conferencing or other forms of entertainment. Use of these devices is only for educational purposes.
- PTDs are not allowed to access the Bedford County Schools regular network in any way.
- Employees are not allowed to use peer-to-peer software, file sharing programs, telnet or messenger programs as well as other resource intensive applications while on the staff network.
- Users must login to the wireless network with a personal network access key or other personally assigned credentials. Users are expected to safeguard their network credentials and not share with other staff members or students. Use of another person's network credentials, with or without the account owner's authorization, is strictly prohibited and could result in loss of network privileges.

- PTDs shall not impair the security of the staff wireless network which means that users are expected to maintain up to date anti-virus, anti-malware and anti-spyware protection on all devices that are connected to the network. Devices without up to date security programs may be denied access to the network.
- Users may not create unauthorized wireless networks to access the BOE-Staff network. This includes establishing wireless access points, wireless routers, and open networks on personal devices.
- Users are responsible for setting up and maintaining their devices. The district will not provide technology support for these devices. Neither technician nor school liaison will work on such devices.
- Users should not intentionally interfere with the performance of the wireless network and/or the district's overall network.
- The BOE-Staff wireless network will not provide print services or district instructional software that is not web-based outside the network.
- Users can be held accountable for any damage to any network caused by employee's personal device or actions.
- Users will not allow any student at any time to access or use the employee's personal technology device.
- Use of personal devices should not interfere with or impair an employee's job performance nor advance personal profit.
- Connectivity may be limited or denied during peak usage times such as online testing windows.

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.

Employee Name: _____
(Please Print)

Employee Signature: _____ Date: _____

School: _____