

## Personnel

**SUBJECT: STAFF USE OF PERSONAL/MOBILE TECHNOLOGY**

All staff who use mobile technology in the course of their job duties, including but not limited to cell phones, smart phones, flash drives, tablets, e-readers, laptop computers, scanners, printers, digital cameras, camcorders, PDAs, iPads and iPods, shall abide by this Regulation which governs the use of this type of equipment. Any device that runs software or systems including, but not limited to, Palm OS, Windows, Pocket PC, Android or IOS is considered a "computer" for the purposes of this Regulation. In addition, all applicable language in Policy and Regulation #6410 and #6410R -- Staff Use of Computerized Information Resources and Form #6410F -- Agreement for Staff Use of Computerized Information Resources (AUP) also applies to mobile and personal technology equipment when it is used in conjunction with the BOCES wireless network or in the course of the staff member's job duties.

Access to confidential data is a privilege afforded to BOCES staff in the performance of their duties. Safeguarding this data is a BOCES responsibility that the Board of Education takes very seriously. Consequently, BOCES employment does not automatically guarantee the initial or ongoing ability to use mobile/personal devices to access the BCS and the information contained therein.

**Confidentiality and Private Information and Privacy Rights**

Confidential and/or private data, including but not limited to, protected student records, employee personal identifying information, and BOCES assessment data, shall only be loaded, stored or transferred to BOCES-owned devices which have encryption and/or password protection. This restriction, designed to ensure data security, encompasses all computers and devices within the BCS, any mobile devices, including flash or key drives, and any devices that access the BCS from remote locations. Staff will not use email to transmit confidential files in order to work at home or another location. Staff will not use cloud-based storage services (such as Dropbox, GoogleDrive, SkyDrive, etc.) for confidential files.

Staff will not leave any devices unattended with confidential information visible. All devices are required to be locked down while the staff member steps away from the device, and settings enabled to freeze and lock after a set period of inactivity.

Staff data files and electronic storage areas shall remain BOCES property, subject to BOCES control and inspection. The Technology Coordinator may access all such files and communications without prior notice to ensure system integrity and that users are complying with requirements of this policy and accompanying regulations. Staff should **NOT** expect that information stored on the BCS will be private.

(Continued)

**SUBJECT: STAFF USE OF PERSONAL/MOBILE TECHNOLOGY (Cont'd.)****Personally Owned Devices**

Staff may use their own personal devices to perform job-related functions only with prior approval from the department's leadership via approval form. If a staff member is permitted to use his/her own personal technology equipment, the following guidelines will apply:

- 1) Prior to use on the BCS or wireless network, all mobile devices must be approved by Technology staff. The BOCES may choose to maintain a list of approved mobile devices and related software applications and utilities. Devices not on the approved list may not connect to the BCS. If a staff member has a device he/she wishes to use and that device is not on the list, he/she must contact the Technology Coordinator. The BOCES and Technology Coordinator reserves the right to update the list as needed.
- 2) The entire cost to acquire all personal technology equipment is the responsibility of the staff member. Services that may incur a financial cost to the BOCES, such as phone options or other "apps" are not allowed. The BOCES does not agree to pay such charges and staff who desire these options must assume all costs incurred for such charges.
- 3) Personal technology equipment is not covered by the BOCES's insurance if it is lost, stolen or damaged. Loss or damage to any personal technology equipment is solely the responsibility of the staff member. If lost or stolen, the loss should be reported immediately to Technology staff so appropriate action can be taken to minimize any possible risk to the BCS and the BOCES.
- 4) Staff assumes complete responsibility for the maintenance of personal devices, including maintenance to conform to BOCES standards. Staff also assumes all responsibility for problem resolution, as well as the use and maintenance of functional, up-to-date anti-virus and anti-malware software and any other protections deemed necessary by Technology staff.
- 5) Staff must also meet any expectations of continuity in formatting of files, etc. when making changes to documents for work purposes (i.e., do not change the format of a file so that the original file is unusable on BOCES-owned hardware/software).

(Continued)

**SUBJECT: STAFF USE OF PERSONAL/MOBILE TECHNOLOGY (Cont'd.)**

- 6) All personal technology equipment used on the BCS or wireless network is subject to review by the BOCES Technology Coordinator, or individuals/entities designated by the Superintendent, if there is reason to suspect that the personal device is causing a problem to the BCS network, or if the staff member is suspected by a supervisor of spending excessive time at work on non-work related matters.
- 7) The BOCES's email client will **not** be installed on personally owned devices. All access to email and personnel forms will be through employee access on the BOCES webpage, or on a BOCES owned device only.
- 8) The use of personal technology equipment in the course of a staff member's professional responsibilities may result in the equipment and/or certain data maintained on it being subject to review, production and/or disclosure (i.e., in response to a FOIL request, discovery demand or subpoena). The staff is required to submit any such information or equipment, when requested.
- 9) It is also the responsibility of BOCES staff using a mobile device, personal or BOCES-owned, to ensure that all security protocols normally used in the management of BOCES data on conventional storage infrastructure are also applied on that mobile device. All BOCES-defined processes for storing, accessing and backing up data must be used on any device used to access the BCS.
- 10) Staff may access the BCS remotely if the staff member has demonstrated that his/her personal device
  - meets the security standards set by the BOCES
  - written prior approval of a supervisor is submitted to the BOCES Technology Department
  - is on the list of approved devices by the BOCES
- 11) Use of any mobile technology device during the school day, whether BOCES-issued or personally owned, should not interfere with the staff member's ability to carry out daily responsibilities.

**BOCES-Issued Devices**

Mobile wireless devices issued by the BOCES will be subject to audit and inventory standards. Staff must be able to produce the device when requested by a BOCES official. If the device is lost or damaged, it must be reported to the staff member's supervisor immediately. If theft is suspected, law enforcement will be contacted.

(Continued)

**SUBJECT: STAFF USE OF PERSONAL/MOBILE TECHNOLOGY (Cont'd.)****Flash Drives**

Flash or key drives may be provided to staff members for use on the BOCES network if required by their job responsibilities. These flash drives will be encrypted and/or password protected. Use of a personally owned flash drive to conduct BOCES business is prohibited.

**Wireless Devices on BOCES Premises**

- 1) For security reasons, staff who use their personal device to connect to the Internet, using a BOCES network, will only be permitted to use the BOCES's staff wireless network. Access to any other BOCES network using a personal device is prohibited.
- 2) Personal devices that have the ability to offer wireless access to other devices must not be used to provide that functionality to others in any BOCES building. The ability to connect personal devices to the BOCES wireless network is a privilege and not a right for staff. Any staff member who violates the conditions of this regulation using his/her own device will have his/her access privileges withdrawn.
- 3) When personal devices are used in BOCES facilities or on the BOCES wireless network, the BOCES reserves the right to:
  - a. Make determinations on whether specific uses of the personally owned wireless devices are consistent with the Staff Acceptable Use of Technology agreement;
  - b. Log network use and monitor storage disk space utilized by such users; and
  - c. Remove or restrict the user's access to the network and suspend the right to use the personally owned computer in BOCES facilities at any time if it is determined that the user is engaged in unauthorized activity, violating the BOCES's Staff Acceptable Use of Technology agreement, or violating the terms of this Regulation.

Adopted  
09/28/2016