SUBJECT: ELECTRONIC DEVICES: BRING YOUR OWN DEVICE

Personal electronic devices are becoming ever more prevalent in our society. Electronic devices are abundantly available in many forms and at increasingly smaller costs to the individual. As such, the Board of Education recognizes the advantages of allowing staff and students the ability to bring in their personal computing devices to the District and to use these devices in support of the educational goals of the district.

Personal electronic devices include but are not limited to personally owned cell phones, tablets, laptops and computers.

Voice Assistants
Voice assistants such as Amazon Echo Dots and Google Home are designed for consumer use, not educational use. Under FERPA, Family Educational Rights and Privacy Act and New York State Education Law 2-d, these devices cannot be used in schools. Our focus is to protect the privacy and security of students' personally identifiable information especially when we are using third-party contractors/vendors such as the Amazon Echo Dot. Both Amazon and Google have a basic business model of collecting data on users to build profiles on them and target them with advertisements. Currently, Amazon does not have documented terms us use/privacy for the use of Echo Dot in schools. Therefore, voice assistants are not allowed in the school setting.

Security Standards
Employees may not use cloud-based apps or backup that allows district-related data to be transferred to unsecure parties. Due to security issues, personal devices may not be synchronized to other devices in employees' homes. Making any modifications to the device hardware or software beyond authorized and routine installation updates is prohibited unless approved by Information Technology Services (ITS). Employees may not use unsecure Internet sites.

To ensure the security of district information, authorized employees are required to maintain the following security standards:

- Owners must ensure that all computers and other devices capable of running anti-virus/anti-malware software have legally licensed anti-virus software (or other appropriate virus protection products) installed and running. Owners should update definition files at least once per week.
- Computer owners must install the most recent security patches on the system as soon as practical or as directed by Information Technology Services (ITS). Where machines cannot be patched, other actions may need to be taken to secure the machine appropriately.
- Computer owners must ensure that their computers are not connected to any other network while connected to CCCSD's network with the obvious exception of Internet connectivity.
- Computer owners agree to immediately report to their teacher or supervisor and CCCSD's ITS department any incident or suspected incidents of unauthorized access and/or disclosure of district resources, databases, networks, etc.

(Continued)

SUBJECT: ELECTRONIC DEVICES: BRING YOUR OWN DEVICE (CONT'D.)

Security Standards (Cont'd.)

- Computer owners agree that they will invoke the screen lock mechanism on their device to prevent unauthorized users access to their device.
  - Passcode of 4 characters be set
  - Passcode will be required for no more than 10 minutes of inactivity on the device
- In case the device is misplaced or stolen, computer owners will insure they have some mechanism to remote wipe their device. This mechanism can be through their carrier vendor and/or through a district Mobile-Device-Manager (MDM) to remote wipe.
- If a device is being used for district purposes, then family and friends should not use this device.

Protection of the Network

ITS reserves the right to restrict certain types of traffic coming into and across the CCCSD network. ITS restricts traffic that is known to cause damage to the network or hosts on it. ITS also may control other types of traffic that consume too much network capacity, such as file-sharing traffic.

By connecting to the network, users acknowledge that a computer or device that exhibits any of the behaviors listed above is in violation of this policy, and the device will be removed from the network until it meets compliancy standards.

Support

While CCCSD provides an integrated and supportive computing environment, it is the responsibility of systems owner to: maintain their computer, install vendor supplied upgrades/patches to their operating system and applications, keep their virus protection definitions up-to-date, and backup critical data.

Technology Support Services will offer limited support for personal computing devices. Owners are expected to use the warranty and support services of the manufacturer and/or vendors that produced and sold their system. ITS manages a Help Desk that owners may consult on a variety of technology-related subjects including network connectivity, virus protection, standard district applications, and general troubleshooting in direct relationship to district based services only.

Users of the district network may be required to authenticate when connecting a device to it. Users may also need to install an agent on their computers before they are allowed on the network. The role of such an agent would be to audit the computer for compliance with security standards as defined in the Security Standards section above.

(Continued)

SUBJECT: ELECTRONIC DEVICES: BRING YOUR OWN DEVICE (CONT'D.)
Software Installation on Personally Owned Equipment

In support of certain academic programs, district purchased software and electronic books may be provided on a temporary or permanent basis to staff and students. When possible, the district will push software to personally owned devices and will be removed when the checked-out time-frame has ended. App and electronic book availability may be limited to only certain supported device systems.

Software Installation on Personally Owned Equipment (Cont'd.)

Enrollment of a personal device in a mobile-device-management (MDM) system may be required by the end-user to support the use of district owned apps and electronic books.

All software purchased by the district and installed on personally owned systems must be used in compliance with all applicable licenses, notices, contracts, and agreements.

Appropriate Use

While in the District, staff and students are expected to exercise the same discretion in using their personal devices as is expected for the use of district devices. District policies pertaining to harassment, discrimination, retaliation, confidential information and ethics apply to the use of personal devices for all school-related activities.

Excessive personal calls, e-mails or text messaging during the school day, regardless of the device used, can interfere with employee and student productivity and be distracting to others. Limited Personal Use of Technology Resources policy (5840.4) applies to employees while in the district regardless of ownership of the device. The Student Code of Conduct applies to all students and should be reviewed for related information on student conduct and use of personal electronic devices.

See Staff Use of Computerized Information Resources (Policy 6470), Student Use of Computerized Information Resources (Policy 7314) and the Student Code of Conduct for additional information.

Expectation of Privacy

Computer owners agree to and accept that access and/or connection to CCCSD's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. As with district-owned computers, this is done in order to identify accounts/computers that may have been compromised by external parties.

(Continued)

SUBJECT: ELECTRONIC DEVICES: BRING YOUR OWN DEVICE (CONT'D.)

Expectation of Privacy (Cont'd.)

Churchville-Chili Central School District has the right, at any time, to monitor and preserve any communications that utilize the CCCSD's networks in any way, including data, voicemail, telephone logs, Internet use, network traffic, etc., to determine proper utilization. Management reserves the right to review, retain or release personal and district-related data on personal devices to government agencies or third parties during an investigation or litigation.

Mobile-Device-Management agents installed on any personally owned device for the purpose of supplying software to the device or to ensure adherence to the security standards listed above will be setup to collect only non-identifiable information from the device. The District MDM will never be configured to inventory personal apps on a device nor will it collect personal call logs, text logs, or message data in anyway.

District Responsibility

Employees are expected to follow applicable state or federal laws or regulations regarding the use of electronic devices at all times.

Employees whose job responsibilities include regular or occasional driving are expected to refrain from using their personal devices while driving. Regardless of the circumstances, including slow or stopped traffic, employees are required to pull off to the side of the road and safely stop the vehicle before placing or accepting a call or texting. Special care should be taken in situations where there is traffic, inclement weather or unfamiliar areas.

Employees who are charged with traffic violations resulting from the use of their personal devices while driving will be solely responsible for all liabilities that result from such actions.

Employees who work in hazardous areas must refrain from using personal devices as doing so can potentially be a major safety hazard.

Upon resignation or termination of employment, or at any time at the discretion of the District, access to district data systems will be revoked.

(Continued)

SUBJECT: ELECTRONIC DEVICES: BRING YOUR OWN DEVICE (CONT'D.)

Disciplinary Action

Violation of this policy may result in disciplinary action according to the law and in accordance with applicable, collective bargaining agreements. Additionally, individuals are subject to loss of CCCSD Information Resources access privileges, civil, and criminal prosecution.

NOTE: Refer also to: Policy #6470 - Staff Use of Computerized Information Resources
Policy #7314 - Student Use of Computerized Information Resources
Policy #5842 – Limited Personal Use of Technology Resources

Family Educational Rights and Privacy Act
NYSED §2-d

Adopted: 8/26/2014
Revised: 10/22/2019