No. 893

BLOOMSBURG AREA SCHOOL DISTRICT
Policy Manual

Section: OPERATIONS

Title: REMOTE ACCESS, MONITORING AND TRACKING OF DISTRICT-ISSUED DEVICES

Date Adopted: 16 March 2015

Date Last Revised:

893. REMOTE ACCESS, MONITORING AND TRACKING OF DISTRICT-ISSUED DEVICES

.1 Definitions

Device – refers to an identified Device issued by the District to a specific District student for use in connection with the District academic program. This includes, but is not limited to, Device issued by the District in connection with the One-to One Device Initiative, Individualized Education Programs and Service Agreements for identified students with special needs, and other educational purposes.

The One-to One Device Initiative – the District initiative to provide every high school student with access to a District-issued Device computer. The major goals of this initiative are to provide students with 21st Century learning environments both at home and in school, and to give all students access to technology resources.

Remote Access of Devices – means a situation where a District employee or agent, using client management software, accesses a Device in the student's possession. Software maintenance, which will download software and configuration changes automatically when a student connects to the BASD-Net with the Device, does not constitute remote access of the Device. Remote access of Device does not include voluntary participation by the Student or other user in web conferences, chat rooms or other web-based activities.

Software maintenance – means any software or configuration changes sent out to each Device, even if it only affects certain Device, that is necessary for the maintenance and security of the BASD-Net and to ensure that only authorized software is installed on the Device.

.2 Repair and Maintenance of Device

Devices are the property Bloomsburg Area School District**.** Students are responsible for the appropriate use of Devices both at school and at home. The care of Device is the student's responsibility. If a Device needs repair, service or other maintenance, students are to report to the Technology Center in their building. Students should not attempt to repair or service their Device. Vandalism to any Device or accessory is strictly prohibited. Students must present school issued picture ID when they bring their Laptop in or pick up from repair.

.3 Remote Access

Device are equipped with the ability to be accessed remotely in the following two scenarios:

a. Technical Problems: In some instances it may be necessary for a school technology staff to access the Device remotely to resolve a technical problem. A student does not need to be asked for permission prior to remote software maintenance or to resolve a technical issue. Software maintenance may involve the correction of altered code or programming and in some cases may remove files from the Device if the files are deemed to be a threat to the operation or security of the BASD-Net or are stored in unauthorized software.

b. Device Reported Missing or Stolen: If the student or parent/guardian believes the Device is missing stolen, a written report of the incident must to be filled out by the student and parent/ guardian and filed with the Building Principal's office. Once the report is filed, the District may initiate the following procedures for reporting Device missing or stolen which provide as follows:

i. Activate Internet Protocol tracking may be used.

.4 At no time will the Device camera be activated remotely nor will screen shots, audio, video or on-screen text be remotely monitored.

NOTE: The School Board may from time to time approve other tracking technologies; however, no tracking technology will be used unless its function and capabilities have been explained to the parent/guardian and student.

.5 Review of Student Files

At no time will any school employee look at or review the student's files and documents stored on the Device except as follows:

After the Device has been returned by the student to the District:

i. At the end of a school year; or

ii. Any other time the student is required to permanently return the Device and has prior notice and adequate opportunity to remove the student's files from the Device;

iii. If the District has a reasonable suspicion that the student is violating District rules or policies, authorized District administrators may take custody of the Device and review student files. “Reasonable suspicion” means reasonable grounds exists that the search will uncover evidence that the student violated the law or school rules or District policies. The scope of the search must be reasonably related to the violation which justified the search. Under no circumstances will a District employee access a Device remotely for the purpose of this subsection b.

iv. In case of a Device reported missing or suspected stolen, pursuant to a signed consent form that clearly and conspicuously sets forth the ability of the District to access or review such files. This consent form shall be supplemental to the agreement for Device use and must be approved by the Superintendent prior to issuance to a parent, guardian or student. Parents/guardians and student must be informed in writing that the failure to sign this form or to otherwise cooperate with the District or an investigating law enforcement agency in connection with the retrieval of the Device may subject the parents/guardians to the cost of the full replacement value of the Device.

v. Teachers and other school personnel may provide assistance to a student in locating that student’s files in the presence of and at the request of the requesting student.

vi. As disclosed in the request for permission for remote access provided to students pursuant to No. 4 above under “Special Rules for District-Issued Devices.”

References:
Policy No. 252B, BASD-Net and District-Issued Devices: Student Use, Rights and Responsibilities
Policies No. 352, 452, 552, Employee Device Security Procedures and Training
Local Board Procedures No. 009, District-Issued Device Responsibility Chart