AP 4005: Employee Personal Digital Device Use

Background:

Employees are expected to adhere to district guidelines related to personal digital device use.

Personal digital devices used in the workplace to conduct work, such as smartphones, tablets, and laptops, may also be used in uncontrolled public environments, and may easily be lost, stolen or damaged. While mobile devices allow employees to communicate and perform their duties remotely, they pose more privacy and security risks than desktop computers used in secure office spaces.

The purpose of this administrative procedure is to provide employees with guidance to minimize the privacy and security risks unique to the use of district-issued mobile devices for work based on current legal requirements, administrative procedures, and best practices.

Procedures:

1. The Secretary-Treasurer will maintain an approved list of positions that warrant the provision of district-issued cell phones.

2. Employees will take security precautions when using and accessing a district-issued personal digital device or mobile device including:

   2.1. Do not share logon credentials or password (or PIN) with anyone and make sure no one can see your logon credentials or passcode (or PIN) as it is entered.

   2.2. Never reusing passwords with other accounts, especially with personal online accounts.

   2.3. Ensure that all apps/software on your district-issued mobile device are up to date unless advised otherwise –

   2.4. Do not allow friends, family members or other third parties to use a district-issued mobile device.

   2.5. Don’t disable the automatic lock on a district-issued mobile device and always lock it if it is left unattended.

   2.6. Don’t pair non-district-issued Bluetooth devices with a district-issued mobile device; and disable the Bluetooth function on your device when not using it.

   2.7. Don’t plug non-district-issued USB devices to a district-issued mobile device.

2.8. Only plug trusted charger cables and power adaptors to a district-issued mobile device.

2.9. Never plug a district-issued mobile device into a public USB port.

2.10. Exercise caution about opening file attachments or clicking on web links in emails.

2.11. Exercise caution about clicking on web links or file attachments in text messages.

2.12. Exercise caution about which internet websites you visit on your district-issued mobile device.

2.13. Secure the district issued phone in a locked drawer/cabinet/with a computer lock cable or when travelling, in the car trunk or use the hotel front desk safe (not a hotel room safe).

3. At no time will the use of any personal digital device invade or infringe upon the personal privacy or safety of any member of the school district community.

4. The district will not tolerate the publication, via computer and/or other multi-media devices, of materials that create, or are likely to create an environment which negatively impacts or causes significant disruption to the district or school.

5. District management reserves the right to access all files and content on personal digital devices connected to district networks to check for inappropriate use.

6. The district accepts no responsibility for theft or damage that may occur to non-district issued personal digital data devices brought to the school or worksite.

7. Any additional roaming fees incurred on a district-issued cell phone for personal business will be billed back to the employee.

8. Digital data devices should not be used when they could pose a security or safety risk, or when they distract from work tasks including while driving or when operating equipment.

9. Personal digital devices are not to be used for surfing the internet or gaming during work hours. Avoid using district-issued cell phones for personal tasks. Avoid using personal cell phones for work tasks. Do not use cell phones to record confidential information.

10. The district assumes no obligation for support of personal equipment, nor will it accept any liability for modifications made to the equipment.