Book

Policy Manual

Section

800 Property

Title

Computers and Mobile Computing Devices; Use of Personal Devices

Code

813.1

Status

Active

Adopted

October 23, 2013

Proposed June 2022

Purpose

The Board may, in its sole discretion, provide computers, laptop computers or other mobile computing devices to employees for the express purpose of enhancing the productivity and operational efficiency of school-based and administrative activities, functions and instruction. Board members may also be provided with District-owned computers, laptop computers and other mobile computing devices for use in their official capacity. Board members and District employees also may choose to use their own devices for District business, subject to the within policy and procedures established by the District.

The District also issues District-owned computer devices to students as a part of its one-to-one device initiative.

The purpose of this policy is to establish general guidelines for the issuance and utilization of all such devices - whether issued by the District or a personal device used for District business - by Board members, management and personnel within the District.

Definitions

Computing Devices shall include desktop computers, workstations, servers, and Mobile Computing Devices.

Mobile Computing Devices shall include, but are not limited to, laptops, iPads, tablets and cell phones.

Users shall mean all Board members, students, management and personnel within the District who use a Computing Device, whether issued by the District or owned by such individual.

District Devices shall mean all Computing Devices owned by the District which has been issued to a User, or to which access has been granted a User, by the District.

Personal Devices shall mean all Mobile Computing Devices owned by a User and used in whole or in part for District purposes.

District Resources shall mean any District-owned networks, email servers, District-owned subscription technology services such as Microsoft 365, student information system (SIS), cloud-based solutions, Teacher Access Center (TAC), and Home Access Center (HAC).

District-Related Information shall mean data, including, but not limited to, Personally Identifiable Information, business, administrative and financial information, intellectual property information, and other information that is not intentionally made generally available by the District on public websites or publications, and it shall also include data in the form of calendars, e-mails, and other applications.

Delegation of Responsibility

The Superintendent or designee shall ensure appropriate dissemination of this policy and corresponding administrative regulations which may be created to District employees.

The Superintendent or designee shall likewise ensure compliance with the Computers and Mobile Computing Device Policy and any applicable administrative guidelines on a continuing basis.

District Devices--Guidelines for Users

All District Devices shall be used for the sole and express purpose of conducting official business and maintaining the operations of the District. Use of all such District Devices is subject to Board Policy 913 – Network Usage and Safety.

A User may be issued a District Device for the performance of specific job-related duties and responsibilities and as determined by the Superintendent or designee only if:

1. The User is a Board member or is in a full-time position and has an "active" employment status; and job-related duties and responsibilities require regular and systematic use of the particular District Device; or

2. The User is required to perform the majority of their duties away from their primary work location; and has a frequent or regular need to perform a

significant portion of their duties during off-hours and on weekends necessitating the need for issuance of a District Device.
3. The User is an enrolled student who has executed the District's Acceptable Use Form.

A User should be issued either a Computing Device or Mobile Computing Device for the performance of their duties, but not both. Exceptions to this policy must be reviewed and approved by the Superintendent or designee before a User is issued multiple District Devices, unless the User has an employment contract that specifies otherwise.

Persons other than Board members and those not directly employed by the District including, but not limited to, volunteers, independent contractors, retired employees, employees hired on a per diem basis or consultants, or employees on extended leave or with an employment status of "inactive" shall not be eligible for the issuance of any District Device.

Although issued to an individual User, all District Devices are considered property of the District and shall be returned upon termination of employment with the District, after reassignment of job duties, after ceasing to be a Board member, after ceasing to be a student, or immediately upon request at any time by an official of the District. District Devices will appear on the organizational unit's Personal Property Inventory List.

All District Devices issued by the District to Users may include the District's software image and any such additional software installed for specific administrative tasks or specific District supported instructional programs. The installation of any other software images or applications on such devices is prohibited.

Users are expected to take all appropriate measures and precautions to prevent the loss, theft, damage and/or unauthorized use of the District Devices, including the following:

1. Keep the District Device in a locked and secured environment when not being used;

2. Do not leave the District Device for prolonged periods of time in a vehicle, especially in extreme temperatures;

3. Keep food and drinks away from all District Devices and work areas;

4. Do not leave the District Device unattended at any time in an unsecured location (e.g., an unlocked empty classroom or office); and

5. Keep the District Device in sight at all times while in public places, such as public transportation, airports, restaurants, etc.

Should a User's District Device be lost or stolen, the User must:

1. Immediately report the incident to their immediate supervisor and the Superintendent or designee (in the case of Users who are Board members, to the

Superintendent) responsible for administration of this policy;

2. Obtain an official police report documenting the theft or loss; and

3. Provide a copy of the police report to their immediate supervisor and the Superintendent or designee (in the case of Users who are Board members, to the Superintendent). If the User fails to adhere to these procedures, the User will be held legally and financially responsible to the District for the replacement of the lost or stolen equipment.

For all warranty and non-warranty repairs and maintenance of all such District Devices, the User must contact the District's Help Desk. All repairs and maintenance will and must be performed in accordance with the District's current repair and maintenance policies and procedures issued by the Superintendent or designee.

The District is under no legal, financial or other obligation to provide for a replacement Computing Device to any User whose device is lost, stolen or damaged.

The District may add security and other tracking technology to any and all District Devices issued by it and any and all such usage is subject to management review, monitoring and auditing by the District. Other audits may be performed on the usage and internal controls subject to applicable laws and regulations.

Non-compliance with this policy or any corresponding administrative regulation will result in appropriate disciplinary action and/or reimbursement of any and all costs to the District.

Use of Personally Owned Mobile Computing Devices for Work-Related Purposes

Users within the District may have the opportunity to use their Personal Devices for District work purposes when authorized in writing, in advance, by such User and the District Administration. Use of all such Personal Devices for District work purposes is subject to Board Policy 913 – Network Usage and Safety.

Personal Device protocols:

1. To ensure the security of District information, Users desiring to use Personal Devices for District business are required to have anti-virus and mobile device management (MDM) software installed on their Personal Devices. This MDM software will store all District-related information, including calendars, e-mails and other applications in one area that is password-protected and secure. The District's IT department must install this software prior to using the Personal Device for District work purposes.

2. Users may only store District-related information on the District cloud networks or District Devices. Users are responsible for ensuring that no student or staff information is saved on their Personal Devices. District reserves the right to request and take possession of Users' Personal Devices for review. Users may

not store District-related information on USB flash drives without authorization. Users may not use cloud-based apps or backup that allows District-related information to be transferred to unsecure parties. Due to security issues, Personal Devices may not be synchronized with other devices in Users' homes. Making any modifications to the device hardware or software beyond authorized and routine installation updates is prohibited unless approved by IT. Users may not use unsecure Internet sites on such Personal Devices.

Restrictions on authorized use of Personal Devices for District-related Matters:

1. While being used for District business, Users are expected to exercise the same discretion in using their Personal Devices as is expected for the use of District Devices.

2. Users who are nonexempt employees of the District may not use their Personal Devices for District work purposes outside of their normal work schedule without authorization in advance from their direct supervisor. This includes reviewing, sending and responding to e-mails or text messages, responding to phone calls, or making phone calls.

3. Users who are employees may not use their Personal Devices for District work purposes during periods of unpaid leave without authorization from the Superintendent or its designee. The District reserves the right to deactivate the District's software applications and access on the employee's Personal Device during periods of unpaid leave.

4. .It is the responsibility of the employee to ensure that family and friends are not accessing District-owned networks and cloud based file locations on Personal Devices.

Privacy/District Access to Personal Device

The District has the right, at any time, to monitor and preserve any communications that use the District's networks in any way, including data, voice mail, telephone logs, Internet use and network traffic, to determine proper use.
The District reserves the right to review or retain personal and District-related information on Personal Devices or to release the data to government agencies or third parties during an investigation or litigation. The District may review the activity and analyze use patterns to ensure that the District's resources in these areas are being use according to this policy and to ensure compliance with other District policies.
Furthermore, no User may knowingly disable any network software or system identified as a monitoring tool.

Lost, stolen, hacked or damaged Personal Devices

1. Users are expected to protect personal devices used for work-related purposes from loss, damage or theft. Users are expected to take all appropriate measures and precautions to prevent the loss, theft, damage and/or unauthorized use of the Personal Devices as are outlined in this policy with respect to District Devices.

2. Users must immediately notify the Superintendent or its designee in the event their Personal Device which is used or has access to District resources is lost, stolen or damaged.

3. Upon resignation or termination of employment or, in the case of Board members upon the expiration of the Board member's term in office, or at any time on request, the User may be asked to produce the Personal Device for inspection. When the Personal Device is requested, all District-related information on Personal Devices will be removed by IT upon termination of employment or expiration of Board member's term in office. District shall require an attestation that the employee or Board member has not retained any District owned managed information or access rights.

General

The official designated by the Superintendent to oversee the implementation of this policy, the issuance of all District Devices and approval of use of Personal Devices within each respective department shall:

1. Maintain direct oversight of the inventory of equipment, service contracts, and internal controls for all District Devices;

2. Maintain a record of access to District resources;

3. Fully enforce the specifications of this policy and other similar IT policies and procedures setting forth the parameters for the eligibility, approval, assignment, utilization, maintenance, and financial oversight of all Computing Devices under their direct control and supervision; and

4. Ensure compliance with administrative regulations and procedures as applicable.

Non-compliance with this policy or any corresponding administrative regulation will result in appropriate disciplinary action and/or reimbursement of any and all costs to the District**.**

Legal

1. 24 P.S. 2401

24 P.S. 510