San Bernardino Community College District

Add the following to the end of the District's Computer and Network Use Administrative Procedure 3720.

BRING YOUR OWN DEVICE

1. Bring Your Own Device ("BYOD") refers to personally-owned technology devices such as computers, laptops, tablets/eReaders, smartphones and other devices ("Devices") used by employees for District purposes to stay connected to, access data from, or complete tasks in their capacity as District employees ("Users").

The District does not require employees to utilize personal Devices. But for those who choose to do so, this procedure provides standards and rules of behavior for the use of personal Devices to access District network resources and information for District business purposes. Users may access District information on personal Devices only in the conduct of District business and as required to perform assigned or authorized District duties.

Most devices are capable of storing large amounts of data that can easily be lost or stolen. The District's interests are to protect District data and information while allowing Users to utilize personal Devices.

In accordance with this and other District policies, personal Devices used for business purposes are to be used in a responsible manner. These procedures are mandatory requirements for any Devices used for District purposes.

2. Compliance with District Policies and Administrative Procedures:

Users understand that the use of Devices for District purposes is subject to the same District rules and regulations with respect to such use as if the Users are using District-owned devices. Users shall abide by applicable laws and policies with respect to access to, use, disclosure, and/or disposal of District information. These policies and procedures include, but are not limited to: Computer and Network Use BP/AP 3720; Electronic Mail BP/AP 3920; Student Records Directory Information and Privacy BP/AP 6040; and Records Retention and Destruction BP/AP 3310.

3. Users are Responsible for all Maintenance of their Device(s)

a. Users acknowledge that they are solely responsible for the configuration, maintenance, troubleshooting and repair of their personal Devices. This includes maintaining original device operating systems and keeping the Device current with security patches and updates as released by the manufacturer.

4. Requirements for all BYODs Accessing District network services and District information.

b. Users shall not download, transfer or store "Sensitive Business Data" on their Devices. "Sensitive Business Data" is defined as documents or data that is not publicly available and that is protected by laws governing confidentiality of information (e.g., student records FERPA, confidential personnel data, third-party confidential information, etc.). Users shall delete any Sensitive Business Data that may be inadvertently downloaded and stored on the Device (for example, through the process of viewing email attachments sent by others). The District's IT Department will provide Users with instructions for identifying and removing these unintended downloads. Users shall not download/transfer Sensitive Business Data to any non-District device.

c. Users shall password protect Devices using existing password protect utilities available on the User's device. Users shall use strong passwords and keep them well protected. It is recommended that when appropriate, Users choose long password of at least 8 characters and change them periodically. Users shall immediately notify the District's IT Department Help Desk if you believe your passwords have been compromised.

d. Users shall not share the Device with other individuals or family members due to the business use of the Device.

e. Users shall notify the District's IT Department Help Desk at 877-241-1756 if the device is lost or stolen within one hour, or as soon as practical, after you notice the device is missing. If the device is a cell phone or table with District email the District will remotely wipe the device back to its factory settings.

f. If a Device has a remote tracking device, such as the "find my device" option on the iPhone, it should be turned on by the User.

g. Users shall maintain anti-virus (AV) protection on a device when appropriate and possible. Instructions on the recommended AV protection is provided by the District's IT Department.

h. Users shall set an idle timeout that will automatically lock the Device after a period of time. Users should contact their mobile device manufacturer or service provider for assistance.

5. Compliance with Applicable Laws.

Users must comply with federal and state laws that provide further protections to certain types of information, or that may influence how Users handle District information with the Devices. Examples include, but are not limited to:

a. Family Educational Rights and Privacy Act (FERPA) and corresponding Education Code provisions that provide students rights of access to their education records and generally prohibits the disclosure of student education records without the prior written consent of the student.

b. Health Insurance Portability and Accountability Act (HIPAA) which imposes various privacy and security requirements on personal health information collected or maintained by covered entities.

c. Financial Services Modernization Act of 1999 ("Gramm Leach Bliley") and accompanying FTC Standards for Safeguarding Customer Information Requires the District to develop and implement an information security program designed to protect nonpublic personal information gathered and maintained with respect to certain financial activities.

d. The Fourth Amendment to the U.S. Constitution, and various federal and state laws concerning access by law enforcement to information and establishes the procedures and circumstances under which law enforcement authorities may gain access to District data. All warrants, subpoenas, and other legal requests, demands, or orders seeking access to institutional data or systems must be forwarded immediately to the District's Human Resources Department.

e. California Public Records Act provides for public access to District records that are not otherwise exempt from disclosure. All requests for records shall be forwarded to the District's Human Resources Department.

f. California invasion of privacy laws that prohibit the disclosure of personal information about an individual.

g. Civil Discovery and E-Discovery Rules, including the duty to preserve data.