



SDCOE Bring Your Own Device Procedure

San Diego County Office of Education grants its employees use of personally purchased smartphones and tablets at work for their convenience, Bring Your Own Device. SDCOE reserves the right to revoke this privilege if users do not abide by the procedures outlined below.

1. Purpose

This procedure is intended to protect the security and integrity of SDCOE's data and technology infrastructure.

2. Scope

This procedure covers all personally owned wireless devices operating in The San Diego County Office of Education wireless network.

3. Procedure

Personally owned devices are permitted to access any SDCOE network resource available on the public Internet. It is the employees' responsibility to maintain their own device(s) and ensure proper malware/anti-virus software are operational. SDCOE does not manage applications and content on personally owned devices and the employee is personally liable for all costs associated with his or her device.

4. Access

A GUEST wireless network is available for personally owned devices. The GUEST network provides public Internet access only. There is no access to the internal SDCOE network.

The San Diego County Superintendent of Schools (SDCOE) prohibits the use of personally owned computers, tablets, smartphones and all other WiFi enabled devices on its SECURE network.

Note: Other devices connecting to the GUEST Network are not necessarily SDCOE property and may not have sufficient, appropriate or up-to-date anti-virus software installed and running. Connecting to the GUEST Network may expose a device to an infected device. **The user assumes all risk when using the GUEST Network.** SDCOE assumes no liability for any damage or loss of data incurred while using the GUEST Network.

SDCOE defines the SECURE and GUEST networks per the SDCOE "Wireless Network Access Use Procedures" document, located at <https://thehub.sdcoe.net/Intranet%20Documents/PROCEDURE-WirelessNetworkAccessUseProcedure.pdf>.

5. Compliance

SDCOE reserves the right to disconnect devices or disable services without notification.

SDCOE employees and visitors are expected to use personal devices in an ethical manner at all times and adhere to SDCOE Administrative Regulation 3600. SDCOE reserves the right to take appropriate

disciplinary action up to and including termination and/or prosecution for non-compliance with this procedure.

The employee's device may be remotely wiped if:

- 1) The device is lost
- 2) The employee terminates his or her employment
- 3) IT detects a data or procedure breach
- 4) Other security risks

SDCOE reserves the right to disconnect devices or disable services without notification.

It is employee's responsibility to take additional precautions, such as backing up email, contacts, and other important information in an event if IT must remotely wipe the device.

6. Exceptions

Limited exceptions to the procedure may occur due to variations in devices and platforms and must be approved by Assistant Superintendent, Integrated Technology Services.

SDCOE employees must agree to the terms and conditions set forth in this procedure in order to be able to connect their devices to the company network.

7. Revision History

Responsible	Date of Change	Summary of Change