Removable Media Procedures

Removable media (Flash Drives, External Hard Drives, Thumb Drives) is a well-known avenue for data loss and a source of malware infections.

1. Purpose

The purpose of this procedure is to minimize the risk of loss or exposure of sensitive information maintained by The San Diego County Office of Education (SDCOE) and to reduce the risk of acquiring malware infections on computers operated by SDCOE.

2. Scope

This procedure covers all computing devices and servers operating in The San Diego County Office of Education.

3. Procedure

The San Diego County Office of Education staff may only use The San Diego County Office of Education authorized removable media with their devices for work-related functions. Sensitive information generally should not be stored on removable media. If this is required for SDCOE work, it must be encrypted and placed only on officially registered removable media devices. Employees, contractors, and temporary staff will follow all SDCOE data removal procedures to permanently erase SDCOE-specific data from such devices once their use is no longer required. All users agree to immediately report to his/her manager and SDCOE ITS any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of SDCOE resources, databases, networks, etc.

ITS or the Division Administrator will distribute approved Encrypted USB-based memory devices and related software applications and utilities. Devices that are not furnished by ITS or the Division Administrator may not be connected to the SDCOE infrastructure.

4. Compliance

The Integrated Technology Services (ITS) team will verify compliance to this procedure through various methods, including, but not limited to, periodic walk-throughs, business tool reports, internal and external audits, and device restrictions. ITS reserves the right to refuse, by physical and non-physical means, the ability to connect removable media and USB devices to the SDCOE network. ITS will engage in such action if such equipment is being used in such a way that puts the SDCOE's systems, data, users, and clients at risk.

Failure to comply with the Removable Media and Acceptable Use Procedure may, at the full discretion of the organization, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment.

5. Access Control

See sanitation procedure for detailed data wipe procedures for flash memory.

6. Exceptions:

Exceptions to this procedure may be requested on a case-by-case basis and approved by the Assistant Superintendent of Integrated Technology Services.

7. Definitions:

Removable Media - any or all of the following devices and technologies:

- Portable USB-based memory sticks, also known as flash drives, or thumb drives, jump drives, or key drives
- Memory cards in SD, CompactFlash, memory stick, or any related flash-based supplemental storage media.
- USB card readers that allow connectivity to a PC.
- Portable MP3 and MPEG-playing music and media player-type devices such as iPods with internal flash or hard drive-based memory that support a data storage function.
- PDAs, cell phone handsets, and Smartphones with internal flash or hard drive-based memory that support a data storage function.
- Digital cameras with internal or external memory support.
- Removable memory-based media, such as rewritable DVDs, CDs, and floppy disks.
- Any hardware that provides connectivity to USB devices through means such as wireless (WiFi, WiMAX, irDA, Bluetooth among others) or wired network access.

8. Revision History

Responsible	Date of Change	Summary of Change