Responsible: Office of Information Technology

PURPOSE

This Administrative Procedure defines how removable media devices may be used in the Washoe County School District (District) to ensure adherence to the District's Cybersecurity Program.

DEFINITIONS

1. "AutoRun" and "AutoPlay" refer to technologies used to start some programs automatically when removable media is inserted into a computer.
2. "Configuration Management Database" or "CMDB" refers to a centralized tracking system that provides an accurate, detailed, and current inventory of all District IT assets with the potential to store or process District data including devices connected to the District's network physically, virtually, remotely, and those hosted within cloud environments.
3. "Encryption" refers to a procedure used to convert data from its original format to an unreadable or unusable format to anyone without the tools or knowledge needed to reverse the process.
4. "Malware" refers to software of malicious intent such as viruses, worms, or spyware.
5. "Removable Media" refers to a portable device that can be connected to an information system (IS), computer, or network to provide reusable readable and/or writeable data storage. Removable Media may refer to the following:
    a. Portable USB-based memory sticks (flash drives, pen drives, thumb drives).
    b. SD Storage.
    c. Portable media devices with internal drive-based storage (smart phones, iPods, MP3 players).
    d. Digital cameras with memory support.
    e. Optical media (CD, DVD, Blu Ray disks).
    f. Any hardware that provides connectivity to USB devices through wireless.

6. "Sanitization" refers to a process that renders access to target data on the media infeasible. Clearing, purging, or physically destroying are actions that can be taken to sanitize media.

PROCEDURE

1. Removable Media refers to a portable device that can be connected to an information system (IS), computer, or network to provide reusable readable and/or writeable data storage. Removable media inherently introduces system and data security risks because it facilitates easy data transfers in and out of District systems.

2. All District personnel have a responsibility to protect District information that is collected, processed, transmitted, stored, or transmitted using mobile computing devices or Removable Media.

3. All Users should avoid using removable media and instead adopt secure alternatives for data transfer such as District-approved cloud storage that support accountability and attribution.

4. Removable Media is subject to data protection requirements such as FERPA when used to store or process sensitive information.

5. Removable Media must be:

    a. Used only when no other suitable alternative is technically feasible;

    b. Securely provisioned through established District channels;

    c. Centrally tracked and controlled throughout its lifecycle;

    d. Tagged with a District Asset Tag;

    e. Encrypted whenever practicable;

    f. Reported if lost or stolen; and,

    g. Sanitized and disposed of to ensure that the data cannot be reconstructed.

6. Removable Media Ownership.

    a. Removable media devices connecting to District assets must be District-owned and controlled ("District Removable Media").

    b. District Removable Media is not permitted to connect to personally owned devices.

c. Personally-owned removable media is not permitted to connect to District-owned devices and shall not be used to store District data.

7. Removable Media Asset Management.

    a. The Office of Information Technology must maintain an accurate, detailed, and current inventory of all District assets used to store or process District information including District Removable Media.

    b. District Removable Media must be centrally tracked and registered in the Enterprise Configuration Management Database (CMDB).

    c. All users must report their District Removable Media devices to the Office of Information Technology so that they can be entered in the CMDB.

    d. Each Removable Media "Configuration Item" entry in the CMDB must include:

        i. Device make and model;

        ii. Device serial number;

        iii. Asset tag number;

        iv. Asset owner;

        v. Department;

        vi. Information classification; and,

        vii. Whether the device is approved to connect to District devices.

    e. District Removable Media devices must be physically marked with District asset tags to ensure that users can immediately identify the device and understand the importance of protecting it. If the device is too small to be tagged with a conventional asset tag, it may be kept in a case with an affixed asset tag.

8. Removable Media Security.

    a. The Office of Information Technology may implement technologies to prevent data loss by auditing, restricting, or otherwise controlling removable media usage within the District.

    b. Users must ensure that removable storage devices are physically secured by storing devices in protected areas such as locked desks or offices in WCSD facilities.

    c. Users must not leave Removable Media devices unattended in public areas.

d. All District Removable Media must be encrypted and password protected in case of loss where practicable. Users must never store sensitive District information in an unencrypted form on removable media or mobile computing devices.

    i. District data stored on Removable Media must be encrypted with FIPS 140-2 compliant encryption algorithms.

    ii. Passwords used to secure removable media must adhere to requirements defined by Administrative Regulation 7234 – "Authenticators".

e. If a device containing District information is lost or stolen, the incident must be reported to the Office of Information Technology, IT Security Department immediately.

9. Device Configuration.

    a. District Information Systems must be configured to:

        i. Broadly block Removable Media except where necessary;

        ii. Prevent Auto-Run and Auto-Play functionality; and,

        iii. Automatically perform anti-malware scanning of removable media devices upon insertion.

10. Removable Media Disposal.

    a. Removable Media must be sanitized or physically destroyed prior to disposal to prevent any potentially unauthorized access to District information.

    b. Sanitization methods will differ based on the type of removable media.

    c. Media sanitization must occur in accordance with industry best practices, or the established recommendations published in NIST 800-88 r 1, "Guidelines for Media Sanitization."

    d. If the District outsources media sanitization and disposal to a third-party e-waste provider, the vendor must adhere to District established standards for media disposal. Third-party vendors must provide Certificates of "Sanitization" or "Destruction" when disposing of removable media on behalf of the District.

LEGAL REQUIREMENTS AND ASSOCIATED DOCUMENTS

1. This Administrative Procedure aligns and complies with the governing documents of the District, to include:
    a. Board Policy 7205, Information Technology – Data Access Policy;
    b. Board Policy 7210, Information Technology Services and Operations;
2. This Administrative Procedure aligns and complies with Nevada Revised Statutes (NRS) and Nevada Administrative Code (NAC), to include:
    a. NRS Chapter 603A, Security and Privacy of Personal Information.

REVISION HISTORY

Date	Revision	Modification
12/03/2025	1.0	Adopted