LOS ANGELES UNIFIED SCHOOL DISTRICT
POLICY BULLETIN

TITLE: **Data Destruction and Disposal**

NUMBER: BUL-6916.0

ISSUER: Shahryar Khazei, Chief Information Officer
Information Technology Division

James Thurmond, Director of IT Security
Information Technology Division

DATE: August 28, 2017

ROUTING
All Employees
All Locations

PURPOSE: The purpose of this policy is to provide the authorized methods for securely and permanently destroying protected pupil and non-pupil District records.

MAJOR CHANGES: This is a new policy bulletin.

GUIDELINES:

SCOPE

The purpose of this policy is to provide the authorized methods for securely and permanently destroying protected pupil and non-pupil District records, as defined in Bulletin 6825.0 and Bulletin 1077.2. This policy assumes that records scheduled for destruction using the methods herein do not violate other applicable record retention policies, procedures, regulations, laws or Board Rules and do not meet **any** of the following conditions:

- Records that must be retained and exist as the only copy.
- Records that are relevant to a potential or active criminal, civil, or administrative case.
- Records with an outstanding public or parental request to inspect or review
- Records that are required by 3rd parties to perform work on behalf of the District or other authorized educational function.

This policy is applicable to all District units that store, secure, retrieve, publish, and destroy "Protected" information which include, but are not limited to, personally identifiable information, pupil information, surveillance video, permanent/non-permanent records, and sensitive security information. The expected users of this policy are all employees, volunteers, and contractors that support records management.

OBJECTIVES

1. Completely destroy protected District information located on obsolete or repurposed IT equipment before the equipment is recycled, disposed of, salvaged, refurbished, sold or donated to external parties for the purpose of avoiding:
    - Privacy litigation
    - Violations of federal regulations
    - Disclosure of sensitive District business operations
    - Breach of software licensing agreements

2. Reduce the cost of maintaining and supporting storage devices in District data centers by minimizing the amount of unnecessarily archived information.

3. Streamline District operations by reducing the time spent on unnecessary backups and discovery requests.

DEFINITIONS

Cryptographic Erasure (CE): A method of sanitization in which the key used to encrypt the target data target is removed, making recovery of the decrypted target data infeasible.

Degaussing: To reverse the magnetizing field of a disk so that information cannot be physically tracked on the platters making the drive permanently unusable.

Encryption: The process of transforming information using a cryptographic algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as an encryption/decryption key.

Personally Identifiable Information: Any information about an individual that can be used to distinguish or trace an individual's identity (e.g. name, social security number, address, etc.).

Sensitive Security Information (SSI): Critical information that, if publicly released, could be useful to threat agents in exploiting security vulnerabilities. SSI is exempt from disclosure under the Freedom of Information Act and may include, but is not limited to, investigations, detailed floor plans, security incident plans, security training materials, network configuration files and lists of critical technology infrastructure.

Self-Encrypting Drives (SED): A type of hard drive that automatically and

continuously encrypts the data on the drive without any user interaction.

Sanitization: A process to render access to data on media infeasible. Clearing, Purging, and destruction are examples of techniques that can sanitize media.

DISPOSAL AND DESTRUCTION OF EQUIPMENT AND MEDIA

EQUIPMENT

This policy applies to all electronic and hard copy records containing protected District information stored on, but not limited to:

- Self-Encrypting Drives
- Office Equipment
- Network Devices
- Hard Copy Storage
- District-Issued Mobile Phones
- Magnetic Storage Media
- Optical Media
- Flash Memory-Based Media

Self-Encrypting Drives

Self-Encrypting Drives (SEDs) with integrated 'always-on' encryption significantly lowers the chance of unprotected District information being left on devices. After information is encrypted, it can be destroyed by just destroying the media encryption key (MEK) used to initially encrypt the information. This process leaves encrypted text on the media that cannot be deciphered. District data custodians may use this method to quickly sanitize large storage media. However, it must not be used when the drive was encrypted after protected or sensitive District information was stored on the device without having first been sanitized.

Office Equipment

If supported, office equipment such as printers, fax machines, and document scanners must be configured each day to automatically and securely remove queued, unprocessed documents from their internal magnetic or flash-based storage media. Office equipment to be recycled, disposed of, salvaged, refurbished, sold or donated to external parties must have their internal storage media sanitized, using methods authorized herein, and all network configuration information cleared by performing a full manufacturer's reset.

Network Devices

Sensitive security information (SSI) on network devices may be cleared rather than physically destroyed. Network administrators must perform a full manufacturer's reset to clear network devices, such as routers, switches, and access points, to their

default factory settings to destroy SSI. Any removable storage media containing SSI used by network devices must be cleared through methods appropriate to the media type authorized herein.

Hard Copy Storage
Paper records with protected information must be destroyed using shredders that produce strips no wider than 6mm of any length or particles no larger than 320 mm , or must be pulverized/disintegrated using disintegrator devices. Microfilm or other reduced-image photo negatives must be destroyed by burning until the residue is reduced to white ash.

District-Issued Mobile Phones
Due to diversity of mobile devices in District circulation, the methods for properly sanitizing protected or sensitive information on them may vary. Cryptographic erasure is the easiest and preferred method for sanitizing mobile phones. However, if this option is not supported then a full reset to default factory settings must be performed to erase all content and settings.

Magnetic Storage Media
a) *Floppy Disks:* Information on floppy disks must be destroyed by degaussing, incineration, pulverization, or shredding.
b) *Cassettes:* All portions of the magnetic tape should be overwritten one time with known non-sensitive signals.
c) *Hard Drives:* This group of storage media includes SATA, PATA, eSATA, SCSI and peripherally attached drives. Cryptographic erasure is the easiest and preferred method for sanitizing magnetic storage media. However, if this option is not available then these drives may be sanitized by executing vendor-supported SANITIZE commands, degaussing, incineration, pulverization, or shredding.

Optical Media
Protected or sensitive security information on CDs, DVDs, and Blu-Ray discs must be sanitized by incineration or shredding.

Flash Memory-Based Storage Devices
a) *Solid State Drive (SSD):* Protected and sensitive security information on SSDs can be sanitized using the same techniques as magnetic media, except for degaussing.

b) *USB Removable Media and Memory Cards:* Due to diversity of USB media in general circulation, methods for properly sanitizing protected or sensitive information may not be supported or the interface to perform sanitization is not standardized, making it difficult to develop accurate procedures across the District. Protected or sensitive security information must be sanitized by

incineration, pulverization or shredding. Memory cards include SD, SDHC, MMC, compact flash memory, micro-drives, and memory sticks which, may be sanitized using the same techniques as for USB removable media.

RECORD DESTRUCTION LOG

District records of erasure/destruction must be kept for all "Protected" information (please see BUL-1077.02, Information Protection Policy for what constitutes protected information).

Records must include the following:

1. Information about the media
2. Date of erasure/destruction
3. Method of erasure/destruction
4. Person who carried out the process

All sanitization techniques, except degaussing, must be verified before logging successful erasure/destruction events to a destruction register.

Example of a Record Destruction Log

Media	Date of Destruction	Method	Person responsible for Destruction
CCTV footage	7/7/17	Degaussing	(first name and last name)
Duplicate employee W-2 records	8/1/17	Shredding	(company name)

Requirements for Storing Record Destruction Log

Record destruction logs must be stored with the following points in mind:

1. Record name (e.g., Record Destruction Log)
2. Storage location (to be determined by local data custodian)
3. Person responsible for storage (local data custodian)
4. Controls for record protection (logs are read-only; they cannot be deleted or edited)
5. Retention time (five [5] years)

VALIDITY AND DOCUMENT MANAGEMENT

The owner of this document is the Director of IT Security, who must check and, if necessary, update the document at least once a year. When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Number of incidents arising from failure to erase or destroy information in a manner specified in this document
- Number of destroyed devices with sensitive security information for which

no record is kept

AUTHORITY: This is a policy of the Los Angeles Unified School District.

RELATED RESOURCES:

- BUL-1077.2, Information Protection Policy
- BUL-6825.0, Records Retention and Destruction
- California Evidence Code sections 1550, et seq.;
- The California Information Practices Act, Civil Code sections 1798, et seq.
- Family Educational Rights and Privacy Act (FERPA), 34 CFR Part 99
- NIST Special Publication 800-88 Rev. 1, Guidelines for Media Sanitization
- ISO/IEC 27001 standard, clauses A.8.3.2, A.11.2.7

ASSISTANCE: For assistance or further information please contact James Thurmond, Director of IT Security, at (213) 241-1707.

ATTACHMENTS: None.