Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Media Sanitization Policy:

PURPOSE:
Clarendon College's policy is that all data must be removed from devices and equipment capable of data storage, transmission, or receipt before equipment disposal.

The technical support staff will properly sanitize information technology resources before transferring, selling, or disposing. All devices capable of storing Clarendon College information must be sanitized in a way that will make data recovery impossible.

This document establishes specific requirements for Information Technology media sanitization at Clarendon College. (See Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C (TAC§202))

SCOPE:
The Clarendon College Media Sanitization Policy applies to any data owner, data custodian, system administrator, and Clarendon College-IT staff that installs, operates, or maintains Clarendon College information technology resources.

POLICY STATEMENT:
Before the sale, transfer, or disposal of information technology resources, the technical support staff will take the appropriate steps, per the Clarendon College-IT Media Sanitization Procedures, to remove all data from any associated storage device.

1. Information technology resources shall be sanitized utilizing a method that will ensure data recovery is impossible, such as degaussing, shredding, or destroying the media using a destruction method that will be able to withstand a laboratory attack (e.g., disintegration, pulverization, melting or incineration).

2. If the device is a cell phone or handheld electronic device, remove the subscriber identity module (SIM) and additional memory cards and destroy them per sanitization requirements. Sanitize the unit utilizing a method that will ensure data recovery is impossible.

3. Document the removal and completion of the process with the following information:
   a. Date;
   b. Description of the item(s) and serial number(s);
   c. Inventory number(s);
   d. The process and sanitization tools used to remove the data, or process and method used for destruction of the media; and
   e. The name and address of the organization to which the equipment was transferred, if applicable.

4. Remove the asset from the Clarendon College IT and equipment inventory. Ensure the removal of the asset by providing the information from item 3 to the Clarendon College Comptroller.

5. All steps above will also be followed when the asset(s) are sold to a third party for resale or destruction.

DEFINITION:
Subscriber Identity Module (SIM): This is an integrated circuit (IC) intended to securely store an international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephone devices (such as mobile phones and laptops). SIMs can also store address book contact information and may be protected using a PIN code to prevent unauthorized use.

Related Policies, References and Attachments:
An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at https://www.clarendoncollege.edu/information-technology.
The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on March 27, 2025, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 18, 2025.