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

PURPOSE:

It is the policy of Clarendon College that all data must be removed from devices and equipment that are capable of data storage, transmission or receipt prior to equipment disposal.

Technical support staff will properly sanitize information technology resources prior to transfer, sale or disposal. It is imperative that all devices capable of storing Clarendon College information 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:

Prior to 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 ensure all data is removed 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 utilizing 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 PDA remove subscriber identity module (SIM) and additional memory cards and destroy 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 to for destruction of the media; and
    e. The name and address of the organization to which the equipment was transferred, if applicable.

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.
Reference materials, legal compliance guidelines, and policy enforcement are available in the Policy Compliance Document. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

This policy was approved by the Clarendon College Board of Regents on July 17, 2023, version1.1. This policy was reviewed by Will Thompson, Vice President of IT on July 15, 2023.