Baldwin Wallace University Information Technology Policy

Issued by:	**Information Technology**
Title:	**Media Disposal**
Number:	**ITP-BW-19**
Publish date:	**June 1, 2022**

1.0 Overview

Baldwin Wallace University is hereinafter referred to as "BW". BW authorized user is hereinafter referred to as “user”.

This policy is to outline the proper disposal of media containing data (physical or electronic) at Baldwin Wallace University. These controls are in place to protect employees, students, and alumni. Inappropriate disposal of media can result in data loss and may put students, faculty, staff, and others, as well as the University, at risk.

2.0 Purpose

The purpose of this policy is to protect BW data from unauthorized disclosure. This policy defines the requirements for ensuring BW data are permanently removed from media before disposal or reuse, a process called "media sanitization," and properly disposing of media. The reuse, recycling, or disposal of computers and other technologies that can store data pose a significant risk since data can easily be recovered with readily available tools - even data from files that were deleted long ago or a hard drive that was reformatted. Failure to properly purge data in these circumstances may result in unauthorized access to BW data, breach of software license agreements, and/or violation of state and federal data security and privacy laws.

3.0 Scope

This policy applies to all information processing/computer systems owned by BW or managed by those entrusted by BW to Third-Parties and Cloud Services as well as end-users of those systems and any information they have transferred into their possession either electronically or on paper. For non-BW managed systems, the requirements in this document must be addressed with Third-Parties in contracted service agreements. See ITP-BW-16 Outsourcing Policy for more details.

4.0 Policy

When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, print-outs, and other similar items used to process, store and/or transmit BW data shall be properly disposed of per measures established by BW.

4.1 Disposal

Physical media, such as print-outs that contain confidential information as defined by ITP-BW-04 Data Classification Policy, shall be disposed of by one of the following methods:

- Shredding using BW-issued shredders.
- Placement in locked shredding bins for a shredding service to properly dispose of.
- Incineration using BW incinerators.

All electronic media and IT systems (hard drives, tape cartridges, CDs, flash drives, printers, copier Hard-drives, etc.) that have been used to process, store, or transmit BW information shall not be released until the equipment has been sanitized and all stored information has been cleared using one of the below methods.

- Overwriting Disk (at least three times) - an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located.
- Degaussing - a method to magnetically erase data from magnetic media. Two types of degaussing exist, strong magnets, and electric degausses. Note that common magnets (e.g., those used to hang a picture on a wall) are relatively weak and cannot effectively degauss magnetic media.
- Destruction – a method of destroying magnetic media. As the name implies, the destruction of magnetic media is physically dismantled utilizing crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be pulled.

4.2 Applicability of Other Policies

This document is part of BW's cohesive set of policies. Other policies may apply to the topics covered in this document, and, as such, the applicable policies should be reviewed as necessary.

5.0 Enforcement

5.1 Employee Enforcement

This policy will be enforced by the Chief Information Security Officer, Chief Information Officer, and BW Administration. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of BW property (physical or intellectual) are suspected, BW may report such activities to the applicable authorities.

5.2 Student Enforcement

Suspected misuse of the facilities should be reported to the Chief Information Security Officer (CISO) or the Chief Information Officer (CIO). The CISO and/or CIO, who is authorized to determine if there has been a violation of policy or law and refer student violators to the Office of Student Conduct for resolution. Pending the outcome, access to the shared technology resources may immediately be restricted or suspended. In some cases, limited access will be provided to the facilities needed for University-related activities, such as classes. Violations can result anywhere from Conduct Probation to suspension or expulsion from the University. Where illegal activities or theft of BW property (physical or intellectual) are suspected, BW may report such activities to the applicable authorities.