Data Destruction and Sanitization Policy

1. Overview

CWL regularly collects sensitive information on computer hard drives and other forms of electronic media. As new equipment is obtained and older equipment and media reach end of life, sensitive information on surplus equipment, and media must be properly destroyed, and otherwise made unreadable to protect confidential information or personally identifiable information (PII).

2. Purpose

Proper disposal and disposition of surplus computer hardware and other storage media, manages risks of security breach and inappropriate information disclosure. Broadly, exposure to the agency takes the form of:

- **Unauthorized Release of Confidential Information or PII (**personally identifiable information**)** - Allowing an unauthorized person access to confidential information.

This policy is designed to address proper disposal procedures for confidential information and/or PII from CWL's waste collections prior to their reuse/recycle. Proper sanitization and disposal procedures are key to ensuring data privacy and license compliance.

3. Scope

This policy applies to all CWL staff.

4. Policy

A. GENERAL

The transfer or disposition of data processing equipment, such as computers and related media, shall be controlled and managed according to ISO 27001 standard guideline's. Data remains present on any type of storage device (whether fixed or removable) even after a disc is "formatted", power is removed, and the device is decommissioned. Simply deleting the data and formatting the disk does not prevent individuals from restoring data. Sanitization of the media removes information in such a way that data recovery using common techniques or analysis is greatly reduced or prevented.

B. DATA DISPOSAL PROCEDURES

All computer desktop's, laptop's, hard drives, and portable media must be processed through CWL's standard operating sanitization procedure for proper disposal. Paper and hard copy records shall be disposed of in a secure manner as specified by the archiving and destruction policy. The Data Sanitization Controller shall ensure procedures exist and are followed that:

All reusable media devices have an integrity test performed to evaluate its final disposition.
1: Failed devices go straight for shredding.
2: Passed devices go straight for sanitization for reuse.

- CWL's Data Sanitization Controller is the managing director

- **Physical Print Media** shall be disposed of inhouse by using CWL's in house paper shredder which has a DIN security level of P-2.

- **Electronic Media** (physical disks, tape cartridge, CDs, printer ribbons, flash drives, printer and copier hard-drives, etc.) shall be disposed of by one of the methods:

    - *Overwriting Magnetic Media* - all devices are over written via Killdisk InfoSec enhanced level 5. Any device that fails to complete must be shredded.

    - *SSD's* (Solid State Drives) and Hybrid drives – Are treated in the same manner as Standard Drives.

    - *Physical Destruction* – items go through CWL's industrial shredder with a maximum shed particle size of 70mm.

IT documentation, hardware, and storage that have been used to process, store, or transmit Confidential Information or PII shall not be released into general surplus until it has been sanitized and all stored information has been cleared using one of the above methods.

5. Audit Controls and Management

CWL document procedures and can provide evidence of practice in the following ways -

- A log of all activity is kept on the Destroyinator's internal hard drive which confirms the state of the drive

- The Destroyinator produces a label that the Data Sanitizing Controller attaches to the corresponding drive, showing drive details i.e. serial number etc. and sanitization result e.g. pass or fail.

- CWL undertake random internal audits to check that the HDD has indeed been wiped. The Data Sanitization controller will select a Hard drive and place it back into the destroyinator and document the findings in the Internal HDD sanitization test log located in the ISO 27001 electronically stored system.

6. Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

7. Distribution

This policy is available for viewing on all staff notice boards and is also held in the ISO 27001 file, and reviewed at least annually

Signed by Nigel Thompson: Date: 19/05/2021

8. Policy Version History

Version	Date	Description	Approved By
1.0	19/12/2017	Initial Policy Drafted	Rebecca Doolan
2.0	20/12/2017	SSD description updated in section in 4. b	Rebecca Doolan
3.0	26/02/2018	Hybrid hard drive included in section 4.b and confidential paper waste service provider amended	Andrea Lee
4.0	10.12.2019	Paper is shredded in house	Andrea Lee
5.0	19.05.2021	CWL no longer have the cross cut shredder, but the more robust industrial paper shredder which has security DIN level P-2. The managing director is the data sanitization controller	Nigel Thompson