Mandatory Secure Erasure and Destruction Controls Policy

Terminology:

Employee or member of staff: someone employed to work for the Business, whether as a fully employed person or as a contractor.

The Business: Web Design UK, or any of its other brand names.

Sensitive information: Includes company data, client data and all data defined in the GDPR.

1. Overview

This policy applies where the Business stores sensitive information on computer hard drives and other forms of electronic media. As old equipment is replaced by new equipment, and media reaches its end of life, Sensitive Information on this equipment and media must be properly destroyed and otherwise made unreadable.

NB. The Business does not generally store sensitive information on its own hardware. Also see section 14.2 in our GDPR policy.

2. Purpose

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

- Violation of Software License Agreements - If software is licensed for use on either a single computer system, to a single person, or to an organisation, licenses are not transferable. If licenses are transferable, there are generally specific requirements that must be met in order to effect a transfer. Allowing a third-party access to licensed software without proper transfer of the license may be a breach of the license agreement, and may subject the Business or the recipient of the software to claims and/or damages.

- Unauthorised Release of Sensitive Information - Allowing an unauthorised person access to Sensitive Information can subject the Business to claims for damages. And subject the employee to Enforcement, see below.

This policy is designed to address proper disposal procedures for Sensitive Information on surplus assets prior to their disposal.

3. Scope

This policy applies to all Business staff.

4. Policy

4.1 General

The transfer or disposition of data processing equipment, such as computers and related media, shall be controlled and managed by the Owner. 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. Sanitisation of the media removes information in such a way that data recovery using common techniques or analysis is greatly reduced or prevented.

4.2 Data Disposal Procedures

All computer desktops, laptops, hard drives, and portable media must be processed through the Owner for proper disposal. Paper and hard copy records shall be disposed of in a secure manner. The Owner shall ensure steps are followed that:

- Organise final disposition of sensitive information, hardware, or electronic media regardless of media format or type.

- Make Sensitive Information unusable and inaccessible, including physical destruction methods to ensure sensitive information is

unusable, inaccessible, and unable to be reconstructed.

- Dispose of Sensitive Information or equipment. Such procedures may include shredding and/or incinerating hard copy materials so that sensitive information cannot be reconstructed. Approved disposal methods include:

    - Physical Print Media shall be disposed of by one (or a combination) of the following methods:

        a) Shredding - Media shall be shredded using [LEP] issued cross-cut shredders
        b) Incineration – Materials are physically destroyed

    - 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:

        a) Overwriting Magnetic Media - Overwriting uses a program to write binary data sector by sector onto the media that requires sanitisation
        b) Physical Destruction – implies complete destruction of media by means of crushing or disassembling the asset and ensuring no data can be extracted or recreated

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

5. Enforcement

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