

# Data Disposal Policy

---

## Contents

Purpose.....	1
Covered records.....	1
Basic principles.....	1
Disposing of paper information.....	2
Disposing of electronic information.....	2

## Purpose

The purpose of this Data Disposal Procedure is to ensure that MENU disposes its official records safely and securely to minimise any unwanted disclosure. This Policy provides procedures for the secure disposal of confidential information.

## Covered records

This Policy applies to all official records generated in the course of the MENU operations, including but not limited to:

- Typed, or printed hardcopy (i.e., paper) documents;
- Electronic records and documents (e.g., email, Web files, text files, PDF files);
- Video or digital images;
- Graphic representations;
- Electronically stored information contained on network servers and/or document management systems; and
- Recorded audio material.

## Basic principles

1. Appropriate procedures must be followed when disposing of information, whether it is in paper or electronic form, to minimise the risk of unwanted disclosure;
2. Precautions must be taken when control of a device that may have information stored locally is to be reassigned to someone else;
3. When devices that store confidential information are to be repaired, then that information must first be removed;

4. Locally installed licensed software must be removed from IT equipment before disposal or transfer of control.

### **Disposing of paper information**

Dispose of unwanted paper documents that do not contain any confidential information by recycling.

Where documents contain confidential information, assess whether the disclosure of the information could cause harm. If so, or if you are uncertain, shred the documents so that they become inisable using one of the shredders placed in the office.

### **Disposing of electronic information**

MENU works with an approved contractor to recycle redundant IT equipment. If employees no longer need an IT equipment provided by MENU, it must be returned to IT administator of MENU, who will securely dispose of the IT equipment.

MENU removes locally stored confidential information as appropriate before a device is assigned to another employee. This must be done routinely at the time the device is returned using a secure file or drive level deletion tool.

The standard method of deleting a data files, on many types of systems, may leave its contents recoverable. This is helpful if a mistake has been made, however, it is insecure if the intention is to prevent anyone else being able to “un-delete” and read the file. As such confidential data is to be deleted permanently by the IT administrator of MENU.