**Clear Desk Policy**

**Template**

This is an example policy. Please ensure you update this policy template so that it’s suitable for your organisation.

## Overview

To improve the security and confidentiality of information, <Organisation> has adopted a Clear Desk Policy for computer and printer workstations.

This ensures that all sensitive and confidential information is properly locked away or disposed of when a workstation is not in use. This includes whether the information is on:

* paper
* storage device
* hardware device

The Clear Desk Policy will reduce the risk of unauthorised access. This includes the loss of, and damage to, information during and outside of normal business hours, or when workstations are left unattended.

A Clear Desk Policy is an important security and privacy control.

## Scope

This policy applies to all permanent, voluntary and contracted staff working directly or indirectly for <Organisation>.

## Policy

Whenever a desk is unoccupied for an extended period of time the following will apply:

1. All sensitive and confidential paperwork must be removed from the desk and locked in a drawer or filing cabinet. This includes mass storage devices, such as USB drives.
2. All waste paper that contains sensitive or confidential information must be shredded.
3. Computers must be locked when the desk is unoccupied and shut down at the end of the working day.
4. Laptops, tablets, and other hardware devices must be removed from the desk and locked in a drawer or filing cabinet.
5. Keys for accessing drawers or filing cabinets should not be left unattended at a desk.
6. Printers and fax machines should be treated with the same care under this policy. This means:
	* any print jobs containing sensitive and confidential paperwork should be retrieved immediately – the ‘locked print’ functionality should be used
	* all paperwork left over at the end of the working day will be properly disposed of

## Exceptions

Exceptions to the guiding principles in this policy must be documented and formally approved by the <role> and <organisation>.

Policy exceptions must describe:

* the nature of the exception
* a reasonable explanation for why the policy exception is required
* any risks created by the policy exception
* evidence of approval by all appropriate parties

## Compliance

This policy will be officially monitored for compliance by the <role> and may include random and scheduled inspections.

## Non-compliance

All policies require the participation of staff and volunteers to be successful. Anyone found to have violated this policy may be subject to disciplinary action.

Review of this document: annually by <role>.

Next review date: <date month year>.