Title	**LWETB Clean Desk Policy**
Date	26th May, 2020
Approved	Chief Executive LWETB
Noted By	LWETB Board 26th May, 2020

LWETB Clean Desk Policy

1. Introduction

This policy sets forth the requirements for keeping a clean workspace and ensuring that confidential information and sensitive materials are promptly and securely stored when they are not in use or when the workspace is vacant, preventing unauthorised viewing and access. It applies equally to paper, digital storage media and hardware.

The policy shall apply to all LWETB staff and contractors.

2. Policy

All sensitive/confidential information in the workspace is to be locked away safely when leaving the workspace either during or at the conclusion of the work day.

Computer workstations/laptops must be locked (logged out or shut down) when unattended and at the end of the work day. Portable devices like laptops and tablets that remain in the office overnight must be shut down and stored away.

Mass storage devices such as CD, DVD, USB drives or external hard drives are not recommended as storage media. If used in exceptional circumstances, they must be encrypted and treated as sensitive material and locked away when not in use.

Printed materials must be immediately removed from printers or fax machines. Printing physical copies should be reserved for moments of absolute necessity. Documents should be viewed, shared and managed electronically whenever possible.

All sensitive documentation and confidential information that does not need to be retained with official LWETB records must be placed in the designated shredder bins for destruction, or placed in the locked confidential disposal bins. Placing such items in unlocked, unsealed shredding bags or in boxes marked ‘for shredding’ is not an acceptable method of securing such material. Please refer to LWETB’s Records Retention policy and Schedule for additional information.

File cabinets and drawers containing sensitive information must be kept closed and locked when unattended and not in use.

Whiteboards containing sensitive or confidential data must be thoroughly erased immediately after use.

The use of sticky notes or tear-out slips from items like telephone call message books should be avoided. Sending email is more secure.

Passwords must not be written down or stored anywhere in the office.

Keys and physical access cards must not be left unattended anywhere in the office.

Staff who do not have sufficient lockable storage space for their work documentation and records should bring this to the attention of their line manager.

Managers of sections and departments suffering a shortage of lockable storage should firstly ensure that they are deleting records promptly in accordance with LWETB's Records Retention policy and Schedule, and that they are monitoring and controlling the volume of records being created to ensure that this is not excessive.

If you notice that any of your devices or documents have gone missing, or if you believe your workspace has been tampered with in any way, you must notify the Data Protection Officer immediately.

3. Compliance

It is the responsibility of each staff member to comply with the policy outlined above.

Managers / Principals must verify compliance with this policy through methods including periodic walk-throughs of work areas.

Repeated or serious violations of the clean desk policy can result in disciplinary actions in accordance with LWETB's disciplinary policy.

The Data Protection office is available to give practical assistance with any difficulties complying with this policy.

4. Responsibilities

Owner	**Responsibilities**
Director of Organisation Support and Development	Revisions and updates to the Policy
LWETB Senior Leadership Team	Review of the Policy
LWETB Chief Executive	Approval of the Policy
LWETB Board	Noting of the Policy