# Learning Accord Multi Academy Trust

# Clear Desk and Screen Policy

| | |
|---|---|
| **Version** | **01/25** |
| **Name of Policy Writer** | **EducateHR Ltd** |
| **Last Reviewed** | **January 2025** |
| **Next Review Due** | **January 2026** |

**Contents** **Page**

## 1. Introduction

1.1 This policy sets out best practice for a clear desk and screen protocol by identifying correct procedures to be followed.

1.2 Observation of such procedures and protocols is designed to ensure that all confidential information held either by the academy or, on its behalf, by any of its employees remains protected and secure on a continuous basis.

1.3 Adherence to a clear desk and screen policy minimises the likelihood of such information being left unattended and thus potentially accessible to individuals without appropriate authorisation.

1.4 Adherence to this policy thereby limits the risk of data breach under the General Data Protection Regulation (GDPR) and other relevant legislation.

## 2. Purpose and scope

2.1 The principle aim of this policy is to ensure that confidential or sensitive information about staff, pupils, parents/carers and any other individual or company working for, with, or on behalf of the academy is protected in an appropriate manner.

2.2 To this end, the policy is designed to ensure that relevant data (in whatever format) is, whenever possible, retained out of sight and in a secure manner within a locked area, whether this is physical (for instance a desk drawer) or electronic (for instance a computer screen) and that this will effectively be the case at all times other than when such data is being actively processed.

2.3 The policy is applicable to all members of staff in the academy, including employees, trainees, volunteers, and governors.

2.4 The policy also extends to any other person (such as an external contractor) who may be permitted access to, or who may otherwise become privy to, confidential data belonging to the academy and/or its staff and students etc.

## 3. Objectives

3.1 This policy is intended to establish the minimum requirements for maintaining a clear desk and screen.

3.2 The key principles of adherence to this policy are as follows:

- to demonstrate compliance with GDPR
- to reduce the risk of confidential or sensitive information being accessed or appropriated by unauthorised persons (causing possible reputational damage to the academy as well as leaving it vulnerable to accusations of having breached data protection requirements)
- to inculcate an ethos and culture in which staff are aware of their individual and collective responsibility in relation to the handling and care of confidential data.

## 4. Clear desk procedure

4.1 All members of staff should consider, before printing a hard copy of any document containing confidential or sensitive information, whether it is necessary to do so. Electronic storage may be the safer option in that once hard copy has been created this must be stored securely until being shredded when no longer required.

4.2 All hard copy containing confidential and sensitive information must be secured appropriately by placing such material in a locked drawer or cabinet within the work area whenever members of staff are temporarily absent from their immediate place of work as a result of leaving the room at any point during the working day.

4.3 Similarly, all hard copy containing confidential and sensitive information must be secured appropriately by placing such material inside a locked drawer or cabinet within the work area whenever members of staff leave the premises at the end of each working day.

4.4 Desk drawers, filing cabinets, office cupboards etc are to be kept closed and locked when left unattended if they contain any confidential and/or sensitive information.

4.5 Keys for the locked items of office furniture must not be left unattended and should be kept on the employee's person throughout the working day (unless the individual is absent on annual leave, or is working in a different location, in which event they should be left with a senior member of staff).

4.6 Keys for the locked items of office furniture (or the room(s) in which they are located) are the responsibility of a (designated) member of staff out of working hours (this may be the caretaker or premises manager).

4.7 In the event of unanticipated sickness absence it may occasionally be necessary for keys to be retrieved by the academy (by arrangement with the absent employee or their representative) to gain access to the safe location in which confidential and sensitive information has been secured.

4.8 Regardless of confidentiality, staff must in any case ensure that desks and other workspaces are left sufficiently tidy at the end of each working day to allow cleaning staff to perform their duties.

## 5. Clear screen procedure

5.1 To ensure confidentiality and security of data is observed, all computer screens must either be logged off or revert to a screensaver with robust password protection whenever the staff member operating the computer terminal is away from their work area.

5.2 The academy's IT department will ensure that computer screens which have been inactive for 10 minutes will automatically be locked out and a neutral screensaver displayed.

5.3 In the event of unanticipated sickness absence it may occasionally be necessary for passwords to be retrieved by the academy (by arrangement with the absent employee or their representative) to gain access to the safe location in which confidential and sensitive information has been secured.

5.4 No confidential or sensitive material should be displayed on any computer screen in circumstances that might allow it to be visible to persons unauthorised to view such information (such as visitors to the academy). In the event of such a situation appearing likely computer screens should be cleared and a screensaver displayed.

## 6. Confidential or sensitive material

6.1 No confidential or sensitive material is to be saved to USB or other external drives other than in strict accordance with the academy's Data Protection and E-safety policies, with which all staff members should be familiar.

6.2 Should it be necessary to photocopy any confidential or sensitive material the staff member charged with undertaking this should remain stationed at the printer whilst this task is in progress and should ensure that all copies, as well as the original template, are removed once the process is completed.

## 7. Other policies and procedures

7.1 This policy will be supported by the following policies and procedures:

- Data Protection Policy
- E-safety Policy