



Children's



Endeavour



Trust

# Clear Desk and Clear Screen Policy

The Children's Endeavour Trust comprises:

- Abbot's Hall Community Primary School
- Bosmere Community Primary School
- Broke Hall Community Primary School
- Chilton Community Primary School
- Combs Ford Primary School
- Freeman Community Primary School
- Springfield Junior School
- Whitehouse Community Primary School

## Document Control

<i>Version</i>	<i>Date</i>	<i>Author</i>	<i>Comments</i>
<i>Issue 1</i>	<b>Feb 2024</b>	<b>KW</b>	<i>New policy</i>

**Owner:** DPO

**Approver:** Trust Board

**Statutory Policy:** Yes

**Review Cycle:** 2 years **Approval date:** 28<sup>th</sup> March 2024

## Policy Contents

1. [Purpose and objectives](#)
2. [Scope](#)
3. [Legislation and guidance](#)
4. [Data Protection Principles](#)
5. [Clear desk policy](#)
6. [Clear screen policy](#)
7. [Audits and monitoring](#)
8. [Links with other Policies](#)

## 1. Purpose and objectives

The purpose of this policy is to ensure all staff have an awareness of the importance and best practice of keeping paper, electronic records and documents safe and secure wherever they may be – including, but not limited to:

- IT equipment/monitors and other devices
- Only encrypted external hard drives or USB drives are to be used, which must be stored away.
- Electronic documents including emails, shared drives, SharePoint, photos, audio and video recordings
- MIS, databases and other third-party software/apps.
- Work areas including desk/workstation, offices, classrooms, staffrooms, meeting rooms, photocopier rooms and any other places where personal/sensitive data maybe used or stored.
- Release printing at the point of the printer or collect straight away.
- Removing any paper copies from the printer/ scanner or photocopier.
- Clear away loose paper such as post-it notes.

The outline of this policy is to ensure:

- The confidentiality, integrity and availability of information is adequately protected.
- A reduction in the risk of security breaches through sensitive documents left unattended
- A reduction in the risk of security breaches through unauthorised access to electronic data.

## 2. Scope

This policy applies to all CET staff, trustees, governors, visitors, volunteers and contractors. It also applies to all users whether Trust based, schools or working remotely.

## 3. Legislation

This policy meets the requirements of:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#)
- [Data Protection Act 2018 \(DPA 2018\)](#)
- Guidance published by the Information commissioner's Office (ICO) UK [GDPR](#)

#### **4. Data protection principles**

The UK GDPR is based on data protection principles that our schools and Trust must comply with. The principles say that personal data must be:

- Personal data shall be processed fairly, lawfully and in a transparent manner.
- Collected for specific, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary to fulfil the purpose(s) for which it is being processed.
- Accurate and where necessary, kept up to date.
- Kept no longer than is necessary for the purpose for which it is processed.
- Processed in a way that ensures appropriate security.

#### **5. Clear desk policy**

Documents/files and other media that includes sensitive, confidential and classified information will be secured/locked away whenever they are not in use.

All printing should be release at the time of collection from the printer or MFD or collected straightaway. Documents must not be left in the printer/scanner or MFD.

Desks, classrooms and other work areas/surfaces shall be left clear and tidy at the end of the working day, or when leaving a work area for extended periods:

- All paper, documents, or media that includes personal or sensitive information, confidential and classified shall be stored in a secure/lockable storage (drawers, filing cabinets, cupboards).
- Other documents shall be filed away as appropriate
- Information that is no longer needed, in either paper or electronic form shall securely dispose of or archived – in line with the Trust's retention schedule

Office, classrooms, corridors and other public areas where displays are on view staff must ensure that:

- Sensitive or confidential personal data displayed in classrooms, offices or public areas should not be left visible or displayed to unauthorised persons.
- Personal data (including, but not limiting to for example student and staff lists) shall be stored securely whenever paper or electronic.
- Meeting rooms should have flip charts and whiteboards cleared for the next user. Discarded notes or handouts to be removed.

## 6. Clear screen policy

- When leaving a computer/laptop unattended the screen must **always** be locked (win +L or ctrl-alt-delete, then select lock).
- Switch off computers/laptops at the end of the day.
- Pupil devices such as iPads, Chromebooks and laptops to be put away in a lockable charging trolley at the end of each day, ready for the next user the following day.
- Be aware of the position of your screen(s), wherever possible ensure that they cannot be seen by unauthorised people whilst in use.
- When working from home or from another school. Please ensure any electronic devices such as a laptop is locked when unattended.

## 7. Audits and monitoring

This policy will be audited and monitored by:

- Internal audits and spot checks
- DPO checks and during learning walks
- Feedback to Headteachers. Office managers and to the policy owner.

## 8. Links with other policies

- Acceptable use agreements
- Data Protection
- Data breach
- Online safety
- Privacy notices