



PolyMAT

Clear Desk Policy

Reviewed: November 2023

Approved: December 2023

Revision due: December 2024

Introduction

The Trust aims to implement and maintain data protection measures to ensure that personal data is secured away appropriately to assist in the reduction of risk of unauthorised access, loss and damage to information.

This policy/guidance checklist is designed to give staff assistance on how to secure personal information (both paper and electronic). This policy/guidance applies to all staff including temporary and agency staff.

Good Practice

Staff must abide by the following practice points when handling personal data.

Leaving a room

Whenever a room is unoccupied for an extended period of time, you should do the following:

- Remove all sensitive and confidential paperwork from plain sight and lock it in a drawer or filing cabinet. This includes portable devices such as laptops and tablets.
- Draws should be locked and keys for accessing drawers or filing cabinets should not be left unattended at or near a desk.
- PCs should be screen locked.
- Rooms should be locked.

Confidential waste

- All waste paper which contains sensitive or confidential information must be disposed of either by using the school's onsite secure disposal (shredders) or placed in the designated confidential waste bins.
- Under no circumstances should this information be placed in regular waste paper bins.
- If the school destroy large scale files such as pupil files or HR records, they should be recorded on the data destruction log.

Computer screens

- Devices such as iPads/laptops/Chromebooks/tablets must be locked away at the end of the day.
- Computer workstations must be locked when the desk is unoccupied and completely shut down at the end of the work day.
- Computer/laptop screens are to be locked when left unattended.
- An appropriate passcode/password must be set for all accounts. Passwords must be complex (a mix of letters, numbers and special characters) and must not be shared with others.
- Screens in offices have been arranged to ensure they are not visible to anyone who enters the office space, or if this is not possible will have privacy screens to reduce the likelihood of people accidentally viewing information that they are not supposed to see. It may not always be possible to install a privacy screen. Where this is the case, a notice will be provided at these workstations to advise users to take caution should they wish to process confidential or sensitive personal data in an area which may be visible to others.
- Devices are configured to automatically lock after a period of inactivity.

Displays

- Passwords should not be left in open areas which are visible to others.
- Sensitive or confidential personal data displayed in classrooms should not be left visible or displayed to unauthorised persons.
- Personal data (including but not limited to seating plans, allergy details and student lists) shall be stored in folders or in secure places.
- When sharing screen to the class, staff should ensure that no personal data is shared on the projector and should activate projector mode where possible.
- Before displaying any names and photos, schools will ensure that the student/parent has provided consent.
- Schools will limit the amount of data on displays. If names are necessary, only first names will be used.

Taking data offsite

- You are responsible for the security of the data in your possession and when transporting it off site you must always take steps to keep it secure.

- Paper documents should not be removed from the school without the prior permission of the Trust or School Data Protection Lead. When such permission is given, reasonable steps must be taken to ensure the confidentiality of the information is maintained during transit. In particular, the information is not to be transported in see-through bags or other un-secured storage containers.
- Paper documents should not be used in public spaces and not left unattended in any place where it is at risk (e.g., in car boots, in a luggage rack on public transport).
- Paper documents taken home or printed at home containing personal information, sensitive data and confidential information are not left around where they can be seen, accessed or removed.
- Paper documents are collected from printers as soon as they are produced and not left where they can be casually read.
- The master copy of the data is not to be removed from school premises.
- Paper documents containing personal data are locked away in suitable facilities such as secure filing cabinets in the home just as they would be in the school.
- Documents containing confidential personal information are not pinned to noticeboards where other members of the household may be able to view them.
- Paper documents are disposed of securely by shredding and should not be disposed of with the ordinary waste unless it has been shredded first.

Printing

- Any print jobs containing personal information should be retrieved immediately.
- To release printing the school will use network login credentials or identification cards

Compliance

If you have misplaced any information, then you must let the Trust (for staff in the Central team) or School Data Protection lead know as quickly as possible.

These guidelines will be monitored for compliance by the Trust Data Protection Lead and may include random or scheduled inspections and walkthroughs.