



CLEAR DESK (GDPR) Policy

Our Shared Vision

Striving for excellence in everything we do

High Quality
Education for
ALL

Effective
home/school
and community
partnerships

Equality Mission Statement

We are committed to ensuring equality of educational opportunity and support for all pupils, parents, carers, staff and visitors irrespective of age, sex, race, disability, religion or belief, sexual orientation, pregnancy, gender reassignment, and socio-economic background. We aim to provide a fully inclusive school in which every person feels proud of their identity and is able to participate fully within the school community. We believe that a diverse school community is a strength which should be respected and celebrated by all those who learn, teach and visit here.

Approved by: Site and Financial Management Committee	Date:
Signature (Chair of Committee):	Signature (Headteacher):

Last review date: March 2026	Next review date: March 2027
-------------------------------------	-------------------------------------

This policy covers many of the articles from the UN Convention on the Rights of the Child. Some key ones are listed below.

Article 3 Best Interests of the Child

The best interests of the child must be a top priority in all decisions and actions that affect the child.

Article 6 Life, Survival and Development

Every child has the right to life. Governments must do all they can to ensure that children survive and develop to their full potential.

Document Owner and Approval

The Strategic Business Lead is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the School's policy review schedule.

A current version of this document is available to all members of staff on the school website.

Version History Log

Version	Description of Change	Date of Policy Release by Judicium
1	Initial Issue	06.05.18
2	Updated references to UK GDPR	19.08.21
3	Formatting amendments	03.08.22
4	Included a few additional security measures.	30.08.24

Guidance note

Whilst we refer to this as a 'Clear Desk Policy', the following document can be used as best practice guidance or merely a factsheet that the school are able to use to guide staff as to how they should be keeping and storing physical copies of data throughout the school and specifically, within classrooms and offices.

The measures which we suggest below ensure that there is an appropriate level of data security throughout the school and looks at the various methods in which the school hold personal data, whether this is paper storage, on a device (i.e., a computer) or ensuring that there are physical methods in place to protect data.

Introduction

The School 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 a short period of time, you should do the following:

- Lock your computer (windows L).
- Ensure there is no personal data left on your desk that students could see.

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 mass storage devices such as USB drives and hard drives or laptops and iPads.
- Drawers should be locked and keys for accessing drawers or filing cabinets should not be left unattended at or near a desk.
- Devices should be screen locked and locked away.
- Offices should be locked.

Confidential waste

- All wastepaper 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. The confidential waste bins should be kept in secure areas, away from students.
- Under no circumstances should this information be placed in regular wastepaper 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/USB sticks 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, capital letter, numbers and/or special characters) and must not be shared with 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. If this happens, staff need to report this to the Headteacher as this will be considered a data breach.
- Before displaying any names and photos, the School will ensure that the student/parent has provided consent.
- The School 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 a member of the Senior Leadership Team. 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 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 ID cards..

Compliance

If you have misplaced any information, then you must let the Headteacher know as quickly as possible.

These guidelines will be monitored for compliance by the Strategic Business Lead and may include random or scheduled inspections and walkthroughs.