Clear Desk Policy/Guidance

This is 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 in their rooms.
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 (ie 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 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.

- Draws should be locked and keys for accessing drawers or filing cabinets should not be left unattended at or near a desk.

- Rooms should be locked.

Confidential waste

- All waste paper which contains sensitive or confidential information must be disposed of placed in the designated confidential waste bins.

- Under no circumstances should this information be placed in regular waste paper bins.

P.T.O

Computer Screens

- Computer workstations must be locked when the desk is unoccupied and completely shut down at the end of the work day.
- Computer / laptop screens to be locked when left unattended.

Displays

- Passwords should not be left in open areas which are visible to others.
- Sensitive or confidential personal data displayed in class rooms should not be left visible or displayed to unauthorised persons.
- Personal data (including but not limited to seating plans and student lists) shall be stored in folders or in secure places.

Taking data offsite

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

Printing

- Any print jobs containing personal information should be retrieved immediately.

Compliance

If you have misplaced any information, then you must let Miss Veronica Maher know as quickly as possible.

These guidelines will be monitored for compliance and may include random or scheduled inspections and walkthroughs.

Last review date: May 2024