Title	**GDPR Clear Desk and Screen Policy**
Cross References	**Internal:** • Data Protection Policy • Complaints Policy
Date	**October 2024**

Introduction

This policy has been introduced to contribute to compliance with the General Data Protections Regulations (GDPR) guidelines. The requirements of GDPR are mandatory and Apricot Online takes the issue of Data Protection very seriously.

Information is an asset. Like any other business asset, it has a value and must be protected. Systems that enable us to store, process and communicate this information must also be protected in order to safeguard information assets. 'Information systems' is the collective term for our information and the systems we use to store, process and communicate it.

Personal data is any data that exists in any of the above that can identify a living person e.g. names, photographs, biometrics, CCTV etc. It applies to pupil, parent and staff data.

Paper records containing personal data which are left on desks/workstations overnight or for long periods of time are at risk of theft, unauthorised disclosure and damage. By ensuring that staff securely lock away any these papers at the end of the day, when they are away at meetings and over lunchtime this risk can be reduced.

Security risks of unauthorised access to electronic records are also prevalent when PC screens are left unattended.

Roles and Responsibilities

It is important that all staff understand what is required of them and comply with this policy.

All staff are responsible for ensuring the information on their desk/workstation or screen is adequately protected in compliance with all relevant policies and procedures.

Scope
This policy applies to everyone who has access to the School's information, information assets or IT equipment. This may include, but is not limited to employees of the School.

All those who use or have access to Schools' information must understand and adopt this policy and are responsible for ensuring the security of the Schools' information systems and the information that they use or handle

This policy sets out Apricot Online requirements for each member of staff to protect any documents or records that contain personal data which are kept at their desk/workstation either temporarily or permanently and covers records in all formats including:

- Paper
- Electronic documents
- Emails
- Visual images such as work-related photographs
- Audio and video tapes, CDs, DVDs and cassettes
- Memory sticks
- Laptops/IPADs and portable hard drives
- Databases

Clear Desk Procedure

Personal confidential information must be locked away when not in use and never left unattended. When printing documents containing personal data, ensure that you select an appropriately located printer where you are able to retrieve your printing immediately or use the School's photocopiers with the secure release function. Do not leave personal confidential information for others to find.

An easy way to comply with the clear desk procedure is to work with electronic documents whenever possible – "do you need to print it"?

Ensure documents are disposed of securely. Never put documents containing sensitive, personal or corporate sensitive information in the general waste bins.

All Portable Computing & Data Storage Devices (PCDs) such as USB data sticks, mobile phones and laptops should be encrypted and placed out of sight, preferably locked away at the end of the working day.

Clear Screen Procedure

Always lock the desktop when leaving the workstation/desk unattended.

Pressing CTRL+ALT+DEL and clicking 'Lock this computer' is straight forward and simple. However, a windows key combination is even simpler. Press windows key + L and your computer will lock automatically. (The windows key can usually be found in the bottom left of the keyboard and looks like a flag/window.)

Always be aware of the position of the screen on your workstation. Wherever possible, ensure that it cannot be seen by unauthorised people while in use.

Authorised by: Jodie Butler, Operations Director

Date: October 2024

Review Date: October 2025