# ST PATRICK'S CLASSICAL SCHOOL

# SCHOOL CLEAR DESK/SCREEN POLICY

## Introduction

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

## Rationale

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.

This document should be read in conjunction with the school's GDPR/Data Protection Policy and procedures.

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/staffrooms 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 school 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, Board of Management, temporary workers, partners and contractual third parties.

All those who use or have access to School's information must understand and adopt this policy and are responsible for ensuring the security of the School's information systems and the information that they use or handle.
This policy sets out St. Patrick's Classical schools 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. 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 school sensitive information in the general waste bins (dispose of such documents in the shredding bin located in the school office).

- All Portable Computing & Data Storage Devices 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/Chromebook/Device when leaving the workstation/desk unattended.
- Always be aware of the position of the screen on your workstation. Wherever possible, ensure that it cannot be seen by other staff, students etc. while in use.
- Please use the ‘freeze the screen ‘option for the overhead projector if you are switching between tasks, tabs or documents.
- Always make sure that no open documents on the computer screen are visible to students, visitors, members of the public or colleagues who are not authorised to view them.
- Always use a strong password on all devices to protect school information.

# Compliance:

All members of staff have an obligation to report an actual or potential data protection compliance breach as soon as possible to a member of School Management. Please consult the School Data Protection Polices for further information or speak to a member of management.

The Board of Management review and ratify the School Policy every three years.

Signed:  Signed: 

Fr. Gerry Stuart

Chairperson of Board of Management

Date: 16-11-2026.

Mr. Harry Mc Garry

Principal/Secretary to the Board of Management

Date: 16-11-2026.