D12 Data Security Policy

AIM: St Mary's Catholic School is committed to the safe and secure control and processing of personal data of its students, staff, Governors, applicants, visitors, contractors and other associated persons. This policy sets out the operational mechanisms and organisational procedures that the school uses to protect the security of the information that it controls. This policy aims to provide enough detail for a 'lay-person' to understand and avoids advanced technical descriptions. This policy should be read in conjunction with the school Data Protection Policy.

Definitions:

- '*Personal data'* is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances.
- '*standard'* data refers to the sort of data that a Teacher would usually have in a paper 'mark-book' – e.g. Name, Class, Grades, Codes (e.g. SEN, PP)
- '*sensitive'* data refers to the sort of data that a Teacher would not usually keep in a paper 'mark-book' – e.g. EHCP, Child Protection Records, Addresses, Parental Contact Details. This sort of data requires a higher level of security than '*standard'* data

Where Personal Data is stored

1. There are four main areas[1] in the school where personal data is stored:

   1.1. The School Management Information System (MIS) – The school currently uses SIMS (Capita) for the digital storage of the information on Staff and Students. The information processed by SIMS is stored on the School Server (see point 1.2 below)

   1.2. The School Secure Server – This is a physical server located in a secure area on the school site, which is only accessible by authorised personnel, and currently use RMCC4 Management Software.

   1.3. Digital Data stored on electronic devices, including School Desktop Computers, Laptop Computers and portable storage devices (e.g. USB Memory Stick, External Hard-drive)

   1.4. Hard-copy paper documentation – which are stored in various locations around the school as relevant to the required need.

How Personal Data is secured

2. Each of the areas listed above has its own security controls and protocols to maintain data security, as far as is reasonably possible.

   2.1. The School Management Information System (MIS)

2.1.1. SIMS software is accessible only by authorised staff, and requires a username and password to access.

2.1.2. SIMS is only accessible in the following ways:

2.1.2.1. On a School PC or Laptop

2.1.2.2. Through the SIMS app which can be installed on personal device with the authorisation of the ICT Manager

2.1.2.3. Through the Schools Remote Desktop system (LARA)

2.1.3. The rights/privileges of each member of staff are controlled using the 'System Manager' function that limits the ability to view/edit personal data based on roles that are defined and managed by the ICT Manager.

2.1.4. The personal data that can be view/edited on SIMS is digitally stored on the School Server

2.2. The School Secure Server

2.2.1. The server is in a locked room located in the centre of a building (which would require an intruder to break through at least two doors, and an alarm system to access). Keys for the server room are held only by the ICT Manager and the Site Manager. There are no windows that can be opened. There is an extractor fan in the room, as well as fans on the server to reduce risk of loss by fire.

2.2.2. The server can only be accessed by an authorised user with a login and password with two-factor authentication enabled. The ICT manager is the administrator and only authorised ICT staff have the ability to change settings on the server.

2.2.3. All data-points around the school which connect to the server via the network require an authorised log-in/password so cannot be access by unauthorised personal devices.

2.2.4. The server has an Uninterruptable Power Supply (UPS) to protect against power surges or power loss.

2.2.5. A full system back-up is done weekly, and the back-up tapes are stored in a fire-proof safe in a separate building.

2.2.6. The school server is connected to the HCC Educational Network ("The Grid"). This provides a high level of protection from external threats, (e.g. Firewall protection)

2.2.7. Wireless Connections – The school operates two Wireless Connections (commonly referred to as 'Wi-Fi').

2.2.7.1. The Open Wi-Fi requires a school login and password, so is only accessible by known users

2.2.7.2. The Closed Wi-Fi can only be accessed by authorised school devices and also

requires a
login/password

2.2.8. The Server contains a number or separate storage drives (e.g. Staff, Students, etc.) which can only be accessed by authorised persons (e.g. students can only access their own storage area or the shared 'student' area)

2.2.9. Within the 'Staff Resources' area on the server, access to folders is limited by users (e.g. more sensitive data is accessible only be authorised users)

2.3. Digital Data on electronic devices

2.3.1.All school PCs and Laptops require a username and password to access with two-factor authentication enabled.

2.3.1.1. Staff should not leave a computer unlocked and unattended. Standard set-up of school computers includes an auto-lock function after 5 minutes.

2.3.2. All School PCs and Laptops are protected by the Network protection offered by 'The
Grid' which is managed by Hertfordshire County Council.

2.3.3. Staff who take School Laptops home must take reasonable steps to ensure the security of the device (if it contains or allows access to personal data). These steps should include the following:

2.3.3.1. Ensuring the device is not left unattended while switched on and unlocked

2.3.3.2. Ensuring the device is never left unattended in a public place

2.3.3.3. Keeping the device in a secure location when not in use

2.3.3.4. Staff who use personal Digital storage devices (such as USB Memory sticks) must take reasonable steps to ensure the security of these devices.

2.3.5.For devices that contain 'standard' personal data this should include the following:

2.3.5.1. Never leaving the device connected into a computer unattended.

2.3.5.2. When not kept about your person, the device should be stored in a location which is not normally accessed by un-authorised persons.

2.3.6. For devices which contain 'sensitive' personal data this should also include:

2.3.6.1. Encryption and/or password protection of the device (or relevant folders/documents).

2.3.6.2. When not kept about your person, the device should be stored in a location that requires a key (e.g. Locked Filing Cabinet, drawer, cupboard or office)

2.3.6.3. Staff who use their own personal mobile device to access school files (such as email) must take reasonable steps to ensure the security of the device (if it contains or allows access to personal data). These steps should include the following:

2.3.6.4. Ensuring the device is protected (e.g. PIN, Thumbprint)

2.3.6.5. Ensuring the device is not left unattended while switched on and unlocked

2.3.6.6. Keeping the device in a secure location when not in use

2.4. Hard-copy paper documentation

2.4.1.1. Staff who are responsible for the storage of personal data in paper format must take reasonable steps to ensure the security of the personal data in their respective areas.

2.4.1.2. For 'Standard' personal data this should include:

2.4.2.1. Never leaving the documents unattended in an area that is usually accessed by unauthorised persons (e.g. on a teacher's desk in a classroom)

2.4.2.2. When not kept about your person, the documents should be stored in a location which is not normally accessed by un-authorised persons

2.4.1.3. For 'Sensitive' personal data this should also include:

2.4.3.1. When not kept about your person, the documents should be stored in a location that requires a key (e.g. Locked Filing Cabinet, drawer, cupboard or office)

How is data retained and destroyed

2.5. Personal Data is retained and then destroyed in line with Policy D5 which sets out the recommended retention periods for filing of records.

School Business Committee
Date of Last Review: June 2025
Date of Next Review: June 2026