



ST. MARY'S *Catholic High School, Dubai*

DATA PROTECTION POLICY

2026-2027

DATA PROTECTION POLICY 2026-2027

Purpose and Scope

St. Mary's Catholic High School Dubai formally acknowledges the critical nature of data protection and the statutory rights of individuals concerning the processing of their Personal Data. In the execution of its administrative and educational functions, the institution routinely collects, stores, and processes personal data. The School is strictly committed to managing this data in full compliance with legal safeguards and the stringent operational standards expected of our institution.

All personnel are mandated to adhere strictly to this Data Protection Policy in the execution of their professional duties. Non-compliance with these provisions constitutes a breach of protocol and may result in formal disciplinary proceedings. The Senior Leadership Team bears the ultimate responsibility for enforcing regulatory compliance within their respective operational domains.

AIMS

This policy establishes a mandatory framework to ensure all personal information is processed lawfully, securely, and in strict accordance with relevant United Arab Emirates (UAE) legislation, specifically including Article 379 of the UAE Penal Code, as well as the foundational principles of the UK Data Protection Act 1998 and the EU General Data Protection Regulation (GDPR) 2018.

Under Article 379 of the UAE Penal Code, the unauthorized utilization of a third party's information for personal or third-party advantage, when such information was acquired in the course of professional duties, constitutes a criminal offense.

This policy governs all data irrespective of the collection methodology, utilization, recording, storage, or destruction protocols, and applies equally to physical and electronic records. All personnel involved in the collection, processing, and disclosure of personal data are legally obligated to understand and adhere to these binding directives.

This Data Protection Policy applies universally to all Personal Data processed by the institution concerning current, former, and prospective students (and their parents/guardians), current and former employees, supply chain vendors, and any communicating third parties. This document strictly governs the institutional processing of such data.

Data Protection Terms

For the purposes of this legal framework, the following definitions apply:

- **Data Controller:** The designated legal entity determining the purposes and means of processing Personal Data. In most instances, the School acts as the Data Controller for the information collected during its operational activities.
- **Data Processor:** A third-party organization or individual engaged to process Personal Data strictly on behalf of, and under the explicit instruction of, the Data Controller (e.g., outsourced suppliers and contractors). Internal staff members do not constitute Data Processors.
- **Data Subjects:** The identified or identifiable living individuals to whom the Personal Data pertains.
- **Personal Data:** Any verifiable information relating to an individual who can be identified directly from that information, or from the aggregation of that data with other accessible information. This encompasses nomenclature, identification numbers, geographical addresses (including IP addresses), birth dates, financial or salary records, educational history, professional titles, and photographic imagery. It further includes documented opinions regarding an individual or their conduct. Personal Data encompasses records maintained on physical media, centralized computer networks, or any electronic device, regardless of corporate or personal ownership.
- **Processing:** Any operation or set of operations performed upon Personal Data or Special Category Data. This includes collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure via transmission, dissemination, restriction, erasure, or destruction.
- **Special Categories of Personal Data:** Highly sensitive data classifications requiring enhanced statutory protection measures. This includes data revealing racial or

ethnic origin, political opinions, religious or philosophical beliefs, and trade union membership. It explicitly encompasses health-related data (physical and psychological), genetic data, and biometric data utilized for unique identification purposes. Data pertaining to criminal convictions or associated legal proceedings shall be processed subject to these identical stringent safeguards.

RESPONSIBILITIES

Personal information or data is strictly defined as data relating to a living individual who can be identified from that data, or from other held information.

St. Mary's Catholic High School Dubai is legally accountable for, and must actively demonstrate, the processing of Personal Data in compliance with UAE Data Protection Law (DPL) principles. This constitutes the statutory duty of accountability.

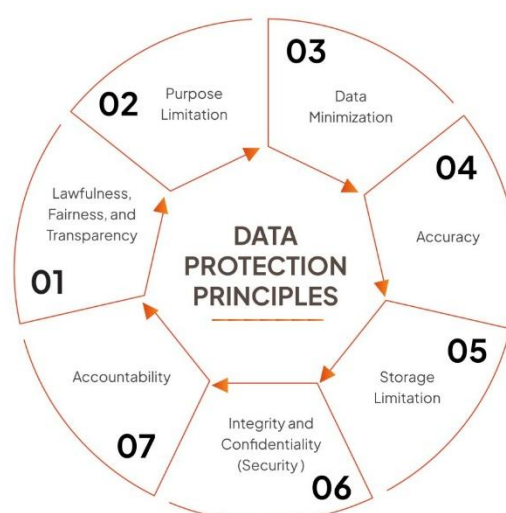
The core principles governing data protection are [NOTE: Based on GDPR principles pending the full promulgation of the UAE Framework]:

- **Principle One - Lawfulness, Fairness & Transparency**



Personal Data must be processed lawfully, fairly, and in a transparent manner. The School shall ensure data is processed exclusively where explicit legal permission exists. The institution commits to transparent disclosure regarding data collection methodologies, utilization purposes, and corresponding legal justifications via formally published Privacy Notices, regardless of whether data is sourced directly from the subject. Furthermore, a systematic assessment of the impact of such processing on affected individuals shall be conducted for all activities. Lawful processing necessitates the satisfaction of at least one of the following statutory bases:

- The Data Subject has provided explicit, freely given, specific, and informed consent.
- Processing is strictly necessary for the execution of a contract to which the Data Subject is a party (e.g., educational provision under the parental contract).
- Processing is mandated by a statutory or legal obligation independent of contractual commitments.
- Processing is imperative to protect the vital interests (life-or-death circumstances) of an individual, such as emergency medical intervention.
- Processing is necessary for the performance of a task carried out in the public interest or under clear statutory authority.
- Processing is necessary for the legitimate interests pursued by the School or a third party, provided such interests are not superseded by the fundamental rights and freedoms of the Data Subject.



- **Principle Two - Purpose Limitation**

Personal Data shall be collected exclusively for specified, explicit, and legitimate purposes, and shall not undergo further processing in any manner incompatible with those original objectives. Processing is restricted to the specific lawful purposes detailed in the Record of Processing Activity and Privacy Notices, barring explicit statutory authorization to the contrary.

- **Principle Three - Data Minimisation**

Personal Data processed shall be strictly adequate, relevant, and limited to the minimum necessary to achieve the stated purpose of processing. The institution ensures a rational nexus between the data acquired and the operational requirement, collecting solely what is imperative for fulfillment.

- **Principle Four - Accuracy**

Personal Data shall be meticulously maintained to ensure accuracy and currency. The School obligates itself to take every reasonable step to ensure that inaccurate data is promptly rectified or erased. Robust procedures govern the verification of data accuracy and the documentation of data sources. The School will formally comply with rights of rectification and thoroughly investigate all substantive challenges to data accuracy.

- **Principle Five - Storage Limitation**

Personal Data shall be retained in an identifiable format for no longer than is strictly necessary for the purposes for which it was originally processed. The School enforces systematic procedures to ensure the secure erasure or destruction of all obsolete data.

- **Principle Six - Integrity and Confidentiality**

Personal Data must be processed with stringent security protocols to protect against unauthorized or unlawful processing, accidental loss, destruction, or damage. The School deploys robust organizational and technical countermeasures to guarantee the confidentiality, integrity, and continuous availability of data processing systems and services.

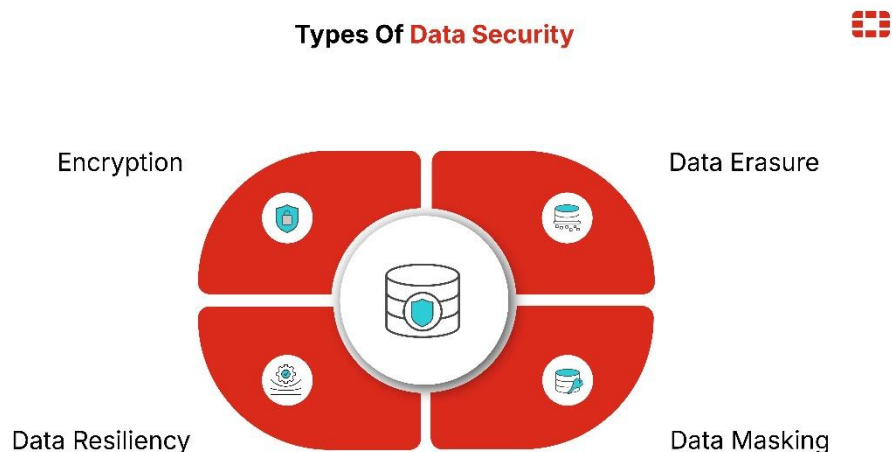
Data Security Protocols

The institution maintains comprehensive security architectures to mitigate risks of unlawful processing, unauthorized access, and accidental data loss. In accordance with Principle Six:

- Confidentiality is enforced by actively preventing unintentional, unlawful, or unauthorized access, disclosure, or misappropriation.
- Integrity is preserved by maintaining data accuracy and preventing unauthorized algorithmic or manual alteration.
- Availability is guaranteed through systematic testing, auditing, and evaluation of technical measures to ensure rapid system restoration in the event of a physical or technical incident.

Authorized institutional security measures include:

- Securing physical records and removable media in locked, restricted-access facilities, followed by certified secure disposal protocols.
- Managing digital records in strict adherence to ratified IT security policies.
- Restricting data sharing strictly to authorized personnel operating within the necessary scope of their professional duties.
- Deploying advanced firewall and IT security infrastructure, subject to recurrent cybersecurity audits.
- Mandating comprehensive data protection and handling training for all personnel.
- Executing periodic audits of institutional governance and information management architectures.



Statutory Notification of Data Subjects

Upon data collection—whether direct or via third-party channels—the School shall issue formal Privacy Notices outlining the following statutory disclosures:

- The designated identity and registered address of the School as the Data Controller.
- The official contact credentials of the Data Protection Lead.
- The specific categories of Personal Data subject to processing.
- The defined operational purposes for said data.
- The applied legal basis for processing (including additional statutory conditions for Special Categories of Data).
- The designated recipients or categories of recipients of the data.
- Protocols governing cross-border data transfers and associated legal safeguards.
- The legally mandated retention period for the data.
- The Data Subject's statutory rights regarding access, restriction, and disclosure.
- The right to lodge a formal complaint with the relevant Regulatory Authority regarding institutional data usage.
- The origin of the Personal Data (if acquired indirectly).
- The utilization of automated decision-making processes, including algorithmic profiling.

Data Subject Rights

The School formally acknowledges and facilitates the statutory rights of Data Subjects, subject to applicable legal caveats. All formal invocations of these rights shall be adjudicated by the Data Protection Lead pursuant to the Information Rights Policy.

- **Right of Access (Subject Access Request):** The entitlement to ascertain processing details, including purpose, recipients, retention periods, and data origin, as well as the right to obtain a formalized copy of the Personal Data held.
- **Right to Rectification:** The entitlement to mandate the correction of materially inaccurate data or the supplementation of incomplete records.
- **Right to Erasure ('Right to be Forgotten'):** The entitlement to request the deletion of Personal Data, applicable exclusively under specific statutory conditions.
- **Right to Object:** The entitlement to prohibit the processing of Personal Data, specifically concerning direct marketing communications or automated decision-making architectures.

- **Rights Pertaining to Automated Individual Decision-Making and Profiling:** The entitlement to object to consequential decisions executed entirely without human intervention, including algorithmic evaluations of personal characteristics. Should the School be legally barred from complying with a request, formal written justification will be provided to the Data Subject detailing the statutory rationale.

Sharing and Transferring Personal Data

The transfer of Personal Data to third-party Data Processors is strictly contingent upon the provision of verifiable guarantees of regulatory compliance and data security commensurate with institutional expectations. Such transfers are strictly governed by legally binding contracts or Data Processing Agreements. The School is authorized to disclose relevant pupil/parent data as operationally necessary to facilitate standard institutional functions. Formal Data Sharing Agreements will be executed with external Data Controllers where legally warranted.

Data Retention and Disposal

The School expressly prohibits the retention of Personal Data beyond its operational necessity, in strict accordance with Principle Five (Storage Limitation). All Personal and Special Category Data shall be destroyed utilizing secure methodologies that guarantee privacy preservation. The School maintains a formal Retention Schedule delineating data classifications and legally mandated retention periods.

Incident Management Procedures

Suspected or confirmed data protection incidents shall be managed through a formalized incident response framework detailed in subsequent sections. Personnel are mandated to adhere strictly to breach reporting protocols, which necessitates the submission of a formalized data incident report for immediate investigation and logging.

Data Protection Impact Assessments (DPIA)

A DPIA is legally mandated prior to undertaking processing activities likely to manifest a high risk to the rights and freedoms of individuals. This proactive risk assessment process identifies vulnerabilities to facilitate the deployment of necessary mitigations or elimination strategies. The School maintains a formal procedural framework instructing personnel on DPIA requirements, including precise guidance on execution thresholds.

CCTV Governance

The deployment of Closed-Circuit Television (CCTV) infrastructure is strictly governed by the School's dedicated CCTV Policy to ensure the lawful collection, processing, and safeguarding of visual data (SIRA).



ST. MARY'S CATHOLIC HIGH SCHOOL DUBAI STAFF

The institution is steadfastly committed to the perpetual enforcement of these data protection principles. Accordingly, the School shall:

- Disclose the operational rationale for data collection at the point of acquisition.
- Notify individuals regarding the circumstances, necessity, and recipients of shared data.
- Conduct systemic reviews of data quality and accuracy.
- Prohibit the excessive retention of data.
- Execute secure and irreversible destruction of obsolete records.
- Implement robust, documented safeguards to prevent loss, theft, or unauthorized disclosure of all data formats.
- Restrict external data sharing exclusively to legally sanctioned scenarios.
- Maintain defined protocols for executing compliance with Subject Access Requests.
- Ensure comprehensive staff awareness and procedural comprehension regarding all policies. Formal grievances shall be adjudicated strictly in accordance with the School's ratified Complaints Policy.

ST. MARY'S CATHOLIC HIGH SCHOOL DUBAI PARENTS

Parents and legal guardians bear the express responsibility of proactively notifying the School of any material changes to their submitted records, inclusive of all primary contact data.



IMPLEMENTATION

Data security compromises can originate from diverse vectors. Recognized breach catalysts include:

- Loss or theft of equipment or media containing pupil, staff, or governing body data.
- Deficient access controls facilitating unauthorized system entry.
- Hardware or system failures.
- Inadequate or non-compliant data destruction protocols.
- Human error or negligence.
- Malicious cyber-attacks.
- Unauthorized system infiltration (Hacking).

Upon the identification or formal notification of a personal data breach, the following emergency protocols must be executed:

- The discovering individual must immediately escalate the incident to the Head Teacher or, in their absence, the designated Deputy Head Teacher and/or the Director of Technology. After-hours discoveries require immediate escalation as soon as is practicable.
- The Head Teacher (or delegated authority) must establish whether the breach is active and ongoing. If active, immediate containment measures must be executed to mitigate operational impact. This may require the emergency suspension of compromised systems and the immediate notification of key operational personnel, such as the Network Operations Manager.
- The institution bears sole responsibility for initiating appropriate corrective action and conducting a thorough internal investigation.
- The Head Teacher (or delegated authority) must evaluate the necessity of law enforcement intervention. This is legally appropriate where illegal activity is confirmed, highly suspected, or poses a future threat. Formal legal counsel should be retained in such scenarios.
- The Head Teacher (or delegated authority) shall execute immediate recovery operations to limit damage and recover losses. Mandated containment actions include:
 - Initiating physical or digital recovery of compromised data or hardware.

- Evaluating the necessity of systemic institutional alerts to personnel. Staff receiving suspicious inquiries must attempt to document the claimant's details, terminate the immediate interaction, and report the occurrence to the Head Teacher (or delegated authority) instantly.
- Executing system restorations utilizing secure back-up archives.
- Liaising immediately with financial institutions to implement fraud prevention measures should financial data be compromised.
- Executing an emergency reset of all compromised access credentials, system passwords, and entry codes, accompanied by mandatory notifications to relevant personnel and oversight agencies.

EVALUATION

This policy framework is subject to mandatory annual review. Formal inquiries pertaining to this policy or the invocation of Subject Access Requests should be directed to the designated contact at itsupport-smchs@smgeducation.org

Approved by: School Management

Review Date :	September 2026
Next Review Date:	August 2027