| INFORMATION & DATA PROTECTION POLICY | | |
|---|---|---|
| **Applicable to** | ☒ Schools ☐ Nurseries | |
| **Teams / Individuals** | ☒ Academic Staff ☒ Administration Staff | |
| **Publishing Channel** | ☒ Parents' VLE ☒ Staff Dashboard ☒ Website ☐ Dept Micro-site | |
| **Linked Policies** | E-Safety & BYOD Policy<br>Safeguarding & Child Protection Policy<br>Complaints Policy<br>CCTV & Footage Viewing & Access Policy | |
| **Linked Documents** | ICO Code of Practice<br>Protection of Freedoms Act 2012<br>UAE PDPL 2021<br>GDPR | |
| **Updated By** | **Latest Publish Date** | **Monitoring Cycle** |
| Dr. Neil Hopkin | 1st November 2025 | Annual |
| **Version No.** | **Amendments** | |
| 1.2 | Formatting, Reference to CCTV & Footage Access & Viewing Policy | |

## RATIONALE

Sunmarke School collects and uses personal information about students, parents, employees, Governors, alumni, and other individuals who come into contact with the school.

This information is gathered to enable the school to provide education and other ancillary functions. In addition, there may be legal requirements from time to time to collect anduse information to ensure that the school complies with its statutory obligations.

This policy is designed to ensure the school operates the highest standards of data governance by which personal information is dealt with correctly, securely and in line with best practice.

The policy applies to all personal information regardless of the way it is collected, used, recorded, stored, and destroyed, and irrespective of whether it is held in paper files or electronically.

This policy applies to all personal information handled regarding current and former employees, suppliers, any third parties interacted with, and prospective, previous, and current students (as well as their parents or guardians).

All staff who process personal data as part of their job are expected to abide by our Data Protection Policy. Infractions of this policy could result in disciplinary action.

## AIM

Sunmarke School ensures all personally identifiable information regarding employees, pupils, parents, governors, guests, and other people is collected, stored, and processed in compliance with the UAE PDPL.

By following these principles, all staff who are engaged in the gathering, processing, and dissemination of personal data will be aware of their roles and obligations.

## LEGISLATION AND GUIDANCE

This policy reflects the:

- Federal Decree Law No. 45 of 2021 on the Protection of Personal Data (the "UAE PDPL"), its amendments and Regulations, as amended from time to time or any other applicable law
- GDPR guidance released by the Information Commissioner's Office (ICO)

Our use of biometric data complies with the Protection of Freedoms Act of 2012.

Our usage of security cameras and private data also mirrors the ICO's code of practice.

## DEFINITIONS

**Personal Data**

Any information relating to an individual that allows identification either directly or indirectly by linking data..

**Sensitive Personal Data**

A sub-category of personal data that directly or indirectly reveals the family ethnicity, racial origin of an individual, philosophical or political opinions, religious beliefs, criminal record, biometric data or data regarding individual health records.

**Data Subject**

An individual who is the subject of personal data. The identified or identifiable person whose personal data is held or processed.

**Data Controller**

A person or organisation who determines the method, criteria and the purpose of processing such personal data.

**Data Processor**

A person or establishment who processes personal data on behalf of the data controller as directed and instructed by the controller.

**Processing**

Any operation or set of operations performed on personal data. This includes collecting, storing, modifying, sharing, disclosing and destroying of personal data.

**Data Breach**

A security incident that has resulted in personal data being lost or stolen, destroyed without consent, changed without consent, or accessed without permission.

- **Confidentiality breach** – is where there is unauthorized or accidental disclosure access to personal data.
- **Availability breach** – is where there is accidental or unauthorized loss of access to or destruction of personal data.
- **Integrity breach** – is where there is an unauthorised or accidental alteration of personal data.

## RESPONSIBILITIES

**All Staff**

All staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy.
- Informing the School of any changes to their personal data, such as a change of address.
- Contacting the Principal in the following circumstances:
    - They have any concerns that this policy is not being followed
    - They are unsure whether or not they have a lawful basis to use personal data in a particular way
    - They need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UAE
    - There has been a data breach
    - They are engaging in a new activity that may affect the privacy rights of individuals

## APPLICATION

Data protection law applies to:

- Data subjects who reside in or work within the UAE.
- Data controllers and processors located in the UAE.

Data Protection Law does not apply to:

- Government data
- Government authorities
- Personal data held by security or judicial authorities.
- Individuals who process their data for their personal purposes
- Personal health data that is subject to separate legislation
- Personal banking and credit that is subject to separate legislation.
- Companies in UAE free zones that are subject to their own personal data related legislation.

## CORE PRINCIPLES AND REQUIREMENTS

The school will adhere to the following core principles in the collection, storage, use, sharingand destruction of personal data:

- Personal data shall be processed fairly and lawfully.
- Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant, and not excessive in relation to thepurpose or purposes for which it is processed.
- Personal data should be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longerthan is necessary for that purpose or purposes.
- Personal data shall be processed in accordance with the rights of data subjects.
- Appropriate disciplinary action shall be taken against unauthorized or unlawful processing of personal data by employees and against accidental loss or destructionof, or damage to, personal data.

## COLLECTING PERSONAL DATA

**Lawfulness, fairness and transparency**

Sunmarke School will only process personal data based on the six legal reasons to do so under data protection law:

1. The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract
2. The data needs to be processed so that the school can comply with a legal obligation
3. The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
4. The data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions
5. The data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden)
6. The individual (or their parent/carer when appropriate in the case of a student) has freely given clear consent

For special categories of personal data, Sunmarke School will also meet one of the special category conditions for processing which are set out in the UAE PDPL

If Sunmarke School offers online services to students, such as classroom applications, and the school intends to rely on consent as a basis for processing, the school will obtain parental consent where the student is under 13 (with the exception of online counselling and preventive services).

Whenever Sunmarke School first collects personal data directly from individuals, the school will provide them with the relevant information required by data protection law.

**Limitation, minimisation and accuracy**

Sunmarke School will only collect personal data for specified explicit and legitimate reasons. Reasons for collecting data will be explained in the consent request. Individuals will be notified should there be a need to use data for a purpose other than those previously specified, and the school will seek consent as required.

## SHARING OF PERSONAL DATA

Sunmarke School shall not share personal data without prior consent, with the exception of the following cases:

- There is an issue with a student or parent/carer that puts the safety of school staff at risk
- School suppliers or contractors need data to enable the school to provide services to staff and students – for example, IT companies. When doing this, the school shall:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data shared
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working together
- Law enforcement and government bodies legally require the school to share personal data, including:
    - The prevention or detection of crime and/or fraud
    - The apprehension or prosecution of offenders
    - In connection with legal proceedings
    - Where the disclosure is required to satisfy the school's safeguarding obligations
    - Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided
- The school may also share personal data with emergency services and local authorities to assist during an emergency that affects any students or staff

- Where the school is required to transfer personal data to a country or territory outside of the UAE, the school will do so in accordance with data protection law

## RIGHTS OF THE INDIVIDUAL

**Parental requests to see the educational record**

Parents, or those with parental responsibility, who would like to see their child's educational record (which includes most information about a student) must request in writing.

## CCTV

Any enquiries about the CCTV system should be directed to the Principal. Further information is detailed in the CCTV & Footage Viewing & Access Policy.

## PHOTOGRAPHS AND VIDEOS

The school takes photographs and records images and videos during school events. Any materials used for communication, marketing and promotional materials will have written consent from parents/guardians or students aged over 18.

The request for parental consent shall explain how the photograph/video will be used to both parent/guardian and student. Any photo or videos taken by parents/guardians at the school for their personal use shall be at their sole discretion and liability. Photos or videos should not be taken of students unless express permission has been provided.

Uses of photos/videos may include:

- Within the school noticeboards and in the school prospectus, display photos around the school, and the school newsletters.
- Outside of the school by external agencies such as the school photographer, newspapers, and campaigns.
- On our school website or social media pages.

Consent can be refused or withdrawn at any time.

## DATA SECURITY AND STORAGE OF RECORDS

The school will endeavor to protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing, or disclosure, and against accidental or unlawful loss, destruction, or damage.

In particular:

- Papers containing confidential personal data must not be left on office and classroom desks, on staff room tables, pinned to notice/display boards, or left anywhere else where there is general access.
- Passwords that are at least 8 characters long containing letters and numbers are used to access School computers, laptops, and other electronic devices. Staff and students are reminded to change their passwords at regular intervals.
- Staff, students, or governors who store personal information on their devices are expected to follow the same security procedures as for School-owned equipment.
- Whenever the school is required to share personal data with a third party, the school shall carry out due diligence and take reasonable steps to ensure it is stored securely and is adequately protected.

## DISPOSAL OF RECORDS

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where the school cannot or does not need to rectify or update it.

For example, the school will shred or incinerate paper-based records and overwrite or delete electronic files. The school may also use a third party to safely dispose of records on the school's behalf. If the school does so, the school will require the third party to provide sufficient guarantees that it complies with data protection law.

## PERSONAL DATA BREACHES

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, the school staff will follow the procedure set out in Appendix 1.

When appropriate, the school will report the data breach to the Director of Education (DoE) within 24 hours. Such breaches in a school context may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person.
- The theft of a school laptop containing non-encrypted personal data about students

## TRAINING

Data protection for all staff will also form part of induction and continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

## MONITORING ARRANGEMENTS

The DoE is responsible for monitoring and reviewing this policy. This policy will be reviewed and updated on an annual basis to ensure changes are reflected appropriately.

## COMPLAINTS

Any complaints relating to Data Protection will be dealt with in alignment with the School's Complaints Policy.