DATA SAFEGUARDING POLICY

TEC_204.1B

Version 1.1
Table of Contents

Purpose

Singapore American School ("SAS") is committed to safeguarding the privacy and security of personal data entrusted to us. This Data Safeguarding Policy sets out the basis on which SAS may collect, use, disclose or otherwise process personal data in accordance with the Personal Data Protection Act 2012 ("PDPA").

Scope

This policy applies to personal data in the school's possession or under its control, including personal data in the possession of third parties engaged by the school to collect, use, disclose or process personal data on the school's behalf.

Definitions

- Personal Data: Refers to any information that can identify a person, either from that data alone or when combined with other information that the school has access to. Examples of personal data include full names, NRIC numbers, financial details, addresses, academic records, and videos/images[1].
- Processing: Any operation performed on personal data, manually or automatically, including collection, storage, use, disclosure, alteration, or deletion.
- Individual: A natural person, whether living or deceased, who is identified or identifiable from personal data.

Safeguarding of Personal Data

Consent Management

SAS obtains consent from individuals prior to collecting, using, sharing, or disclosing their personal data. Consent is obtained by clearly informing individuals about:

- The specific purposes for data collection;
- The contact details of the school's Data Protection Officer (DPO); and
- The right to withdraw consent at any time.

Parental consent shall be deemed sufficient and legally valid for students under the age of 18.

[1] Personal data does not include:
- Business contact information - such as an individual's name, position, business contact information;
- Publicly available information - such as information published in public registers, directories, media reports;
- Data that has been anonymized such that individuals cannot be identified.

Withdrawal of Consent

Individuals may withdraw their consent for the collection, use, or disclosure of their personal data at any time by submitting a written request to the DPO at data@sas.edu.sg. SAS will cease processing the relevant data within a reasonable timeframe, except where continued processing is required for legal or operational reasons, such as student safety or regulatory compliance.

Purpose Limitation

SAS collects, uses and shares personal data solely for specific purposes that a reasonable person would consider appropriate under the circumstances. Typical purposes include (but are not limited to):

- Delivery of educational programs;
- Ensuring student welfare and safeguarding;
- Employment administration; and
- Event management and school trips.

Notification to Individuals

SAS ensures that individuals are notified about the purposes for which their personal data is collected, used, or shared at or before the point of collection. This notification is provided through clear and explicit statements in relevant forms, contracts, or policies. If there is a need to use personal data for additional purposes not initially disclosed, SAS will notify individuals and seek their consent before proceeding.

Accuracy of Personal Data

SAS strives to ensure that the personal data it collects or is collected on its behalf is accurate and complete. As part of maintaining data accuracy, individuals are expected to confirm the accuracy of information at the time of submission and update any changes to personal details throughout the year.

Data Security

SAS implements robust security measures to protect personal data against unauthorized access, accidental data loss, or destruction, including (but are not limited to):

- Access controls limiting system access strictly to authorized personnel;
- Encryption technologies for sensitive electronic records;
- Perimeter security (firewalls), endpoint security (antivirus software), and regular cybersecurity audits; and
- Mandatory staff training and awareness programs regarding secure handling practices.

Access & Correction of Personal Data

SAS supports individuals' rights to access and correct their personal data in accordance with the PDPA. The DPO will handle these requests transparently, within a reasonable timeframe, and will provide reasons if any such requests are denied.

Retention Limitation

SAS retains personal data for only as long as necessary to fulfill the purpose(s) for which it was collected, or as required by applicable laws and regulations. Once the retention period expires or the data is no longer needed, SAS securely disposes of it in accordance with its retention schedule.

Transfer Limitation

SAS will not transfer personal data to a country or territory outside Singapore unless that country or territory ensures a comparable level of data protection.

Data Breach Incident Management

In the event of a suspected or confirmed data breach, SAS will take immediate action to contain, assess, and mitigate the impact. SAS requires that any suspected or confirmed breaches of personal data be reported to the DPO (data@sas.edu.sg) as soon as possible. SAS will notify affected individuals and relevant authorities as required under the PDPA. All breaches will be documented, and corrective measures will be implemented to prevent recurrence and support continuous improvement.

Accountability

The DPO oversees data protection practices, provides guidance, and addresses queries or concerns from stakeholders. Regular training, audits, and reviews are conducted to maintain data protection standards, and appropriate measures are in place to address and rectify any non-compliance.

Related Protocols

This policy should be read alongside:

- Data Governance Procedures: Provides protocols for managing data incidents, including identification, categorization, response, and compliance with data protection laws.
- Data Management Procedures: Specifies how personal data is collected, used, stored, shared, retained, securely archived, or deleted after its necessary period.
- Cybersecurity Procedures: Specifies the principles for safeguarding IT systems, networks, and data from unauthorized access, breaches, and other threats.

These protocols detail specific implementation procedures supporting this policy's principles and requirements.