TANGLIN TRUST
SCHOOL
EST. 1925

Personal Data Protection Policy

1 Introduction

Tanglin Trust School Ltd and Tanglin Trust School Foundation (collectively "School") is fully committed to maintain integrity of personal data of our students, their families, our staff, and third parties whose personal data the School collects, uses, and controls. We safeguard the personal data entrusted to us and strive to comply with all applicable personal data protection laws and regulations, including the Personal Data Protection Act ("PDPA").

Each employee bears a duty to comply with this Policy in the fulfilment of their responsibilities and obligations in the School.

2 Scope

This Policy establishes the general approach as well as sets the minimum standards to which the School must adhere to. It is applicable to all staff, Governors and authorized third parties collecting, processing, using or disclosing personal data on behalf of the School. Any breaches in the protection of personal data may expose the School to civil or criminal penalties as well as reputational damage.

3 Personal Data

Personal data refers to any data, whether by its own or with other data which the School has or is likely to have access to, can identify an individual. Examples of personal data may include:

a) Name
b) Date of birth
c) National identification number
d) Image (photograph / video)
e) Address (residential / mailing / e-mail)
f) Phone number
g) Biometric data such as retina image and fingerprints
h) Computer's IP address
i) CCTV video footage
j) Medical or health record
k) Credit card number / bank account number / financial information

4 Roles & Responsibilities

The School's Finance and Risk Sub-committee of the Board of Governors ("FRC") is accountable for approval of this Policy and directs the development and maintenance of standards, guidelines and procedures pertaining to this Policy. The FRC has delegated the day-to-day responsibility for overseeing and implementation of this Policy to the Risk and Compliance Director.

4.1 Board of Governors

The Board of Governors ("Board") has oversight of the overall compliance with personal data protection requirements. By demonstrating its commitment in establishing an effective internal control system in compliance with legislation and related regulatory guidelines, the Board plays a critical role in setting a personal data protection culture. To fulfil its duties, the Board must be kept informed of timely information from senior management.

4.2 Leadership Team

The Leadership Team is the senior management of the School and has responsibility for ensuring the existence and an operationally effective data protection framework in accordance with this Policy and that this Policy is updated according to any changes in the legislation or the School's circumstances. The Leadership Team must ensure adherence to implementation of this Policy and in particular for

- incorporating the requirements of this Policy into the other School policies and procedures as applicable;
- designating an individual or individuals as the Data Protection Officer ("DPO"). Deputy DPOs may also be designated where appropriate.

4.3 Data Protection Officer

The Data Protection Officer will:

- inform and advise the Leadership Team, employees and relevant third parties of their obligations in relation to the school's data protection policies and procedures;
- attend to requests from data subjects for access, correction, and updating of personal data, and any other matters relating to their personal data held by the School;
- act as the main point of co-ordination with and attend to requests from third parties and the regulators with respect to matters involving personal data protection;
- keep up to date on data protection matters;
- assist in conducting data protection impact assessments on any projects, systems, tool, processes, or enhancements prior to launch or roll-out; and
- provide appropriate training to all relevant employees, in particular for employees engaged in any activity in relations to data privacy.

The Data Protection Officer may appoint Deputy Data Protection Officers to assist in undertaking the roles and responsibilities of the Data Protection Officer.

The Deputy Data Protection Officers shall include the Director of Technology or his nominee who shall assist in managing the aspects of data protection which involve technology systems and processes, and the Corporate Legal Director or his nominee who shall assist in managing the legal aspects of data protection.

4.4 Risk and Compliance Director

The Risk and Compliance Director shall have oversight of all activities relating to data protection including:

- monitoring of compliance with this Policy and applicable laws and regulations;
- informing the Leadership Team of emerging data privacy risks and compliance initiatives, as well as identifying compliance deficiencies and corrective action to be taken;
- overseeing compliance training programs for all relevant employees; and
- taking appropriate action when breaches of this Policy are identified.

4.5 Employees and Data Intermediaries

All employees and data intermediaries play a vital role in ensuring personal data is properly safeguarded and must comply with applicable laws and regulations. All employees and data intermediaries acting on behalf of the School must ensure that the collection, processing, use, disclosure, retention, and destruction of personal data are consistent with this Policy.

A periodic data privacy risk assessment using a risk-based approach is to be conducted to assess potential privacy impact when new procedures involving personal data are implemented or when changes are made to such processes.

Any data privacy breach or incident identified must be reported to the DPO in accordance with the TTS Data Breach Response Plan and the Risk and Compliance Director will be notified.

5 Three Lines of Defence

The School's Risk Management Framework is based on the three lines of defence risk management model which provides for sound management of risks relating to data privacy. The three lines of defence sets out effective guidelines in relation to functions that own and manage risks, functions that oversee risks and functions that provide independent assurance as outlined below:

5.1 First Line of Defence

Employees including Management and Heads of School and Heads of Departments manage the risk associated with the day-to-day activities on data privacy. This includes the collection, processing, use, disclosure, retention, and destruction of personal data as stipulated in this Policy and applicable law and regulations.

Employees are also responsible for ensuring that appropriate organizational, physical, and technical measures are in place to ensure that any processing of personal data is carried out in accordance with this Policy.

5.2 Second Line of Defence

The Risk and Compliance Director will regularly review the personal data protection framework to ensure its effectiveness and to provide support and guidance to the Leadership Team in ensuring that data privacy risks are adequately managed. In conjunction with the Corporate Legal Director, the Risk and Compliance Director will identify updates on laws and regulations pertaining to data privacy and seek legal advice and assistance on the review of the personal data protection framework where necessary.

5.3 Third Line of Defence

Independent testing should be carried out by qualified third parties via periodic internal audits. The testing should evaluate the adequacy of the overall personal data protection program and assess the procedures applied.

6 The Privacy Principles

Data privacy relates to the lawful and appropriate collection, processing, use, disclosure, retention, and destruction of personal data that has been provided or entrusted to a party according to the agreed purposes. The privacy principles provide a privacy guidance and serves as the basis of protecting the rights of the individuals whose personal data has been provided to the School. The privacy principles are:

6.1 Collection and Consent Principle

Personal data should be collected, used, and disclosed only with the consent of the individual, either express or deemed under the PDPA. Circumstances where the personal data is to be shared with another

party should be communicated to the data subject. There should be legitimate reasons for collecting and sharing personal data, which is to occur in an open and honest manner.

Before collection of personal data related to an enrolment of a student and an enquiry or application therefore, the data subject must be provided and indicate agreement to the School's "Personal Data Collection Statement".

Before collection of personal data related to employment or potential employment, the data subject must be provided and indicate agreement to the School's "Personal Data Collection Statement (Employee)".

In all other circumstances where personal data is collected, the staff responsible shall ensure that the data subject is provided with a statement that includes the purpose of collection, the classes of persons to whom the data may be transferred, the consequences of failing to supply the data and the right of access to and correction of the data.

In the event that the use of personal data is not in line with the original specified purposes, valid consent must be obtained anew on the change of purpose unless otherwise provided by law.

On giving reasonable notice to the School, an individual may at any time withdraw any consent given, or deemed to have been given under the PDPA, for the School's collection, use, disclosure, or retention of their personal data. Upon receiving a notification from the individual, the School shall inform the individual of the likely consequences of withdrawing their consent. Upon withdrawal of consent, the School shall cease and notify the School's data intermediaries and agents to cease such collection, use, disclosure, or retention of personal data, as the case may be, unless the continued collection, use, disclosure, or retention of personal data is required or permitted by the PDPA or any other written law.

6.2 Limitation of Purpose Principle

Personal data should only be collected, used, or disclosed for purposes which the individual has expressly consented to or deemed to do so under the PDPA, unless there are applicable exceptions under the law. The purposes of such collection, use or disclosure must be considered appropriate under the circumstances by a reasonable person. We must not collect, use, or disclose personal data for purposes which are different from the original purposes consented to until consent from the individual has been obtained on the proposed new purposes, unless there are applicable exceptions provided under the law. The type and amount of personal data collected, used, or disclosed should not be excessive or more than what is required for the purposes for which they were collected, used, or disclosed. Only personal data necessary to properly fulfil the purpose of collection should be obtained and retained.

6.3 Notification Principle

The individual whose personal data is being obtained must be notified at time of collection of the purpose for which the personal data is collected, processed, used, retained, and/or disclosed.

6.4 Accuracy Principle

Personal data shall be reasonably accurate and complete and, to the extent necessary for those purposes, be kept up-to-date. The data should be correct and not misleading. This, however, excludes circumstances where inaccurate data has been provided by either the individual or a third party.

6.5 Retention Limitation Principle

Personal data collected for any purpose should not be kept longer than is necessary for business or legal purposes and when the purpose for which that personal data was collected is no longer being served by retention of the personal data. The personal data shall either be safely destroyed or anonymised such

that it can no longer be associated with any individuals. A system should be in place for a systematic approach to review and destroy data in both physical and electronic format.

6.6 Access and Correction Principle

Individuals whose personal data are held by the School should have certain rights in relation to their data which include the following, unless covered by exceptions or prohibitions under the law: -

- Right to request for their personal data under the possession or custody of the School;
- Right to request correction or destruction of their data;
- Right to be informed how their personal data was used by the School in the preceding 12 months.

The School is required to provide the information as soon as reasonably possible and in any event no later than 30 days after receiving such data access request. In the event such request cannot be fulfilled within the 30-day period, the School must notify the individual making such request in writing and inform when the information will be provided.

Consult the Corporate Legal Director on whether any exceptions or prohibitions apply to each request.

Requests for access and correction or for information regarding policies and practices and kinds of data held by the School should be addressed in writing to:

Data Protection Officer
Tanglin Trust School
Email: DataProtection@tts.edu.sg

A reasonable fee may be charged to offset any administrative or actual costs incurred in complying with such data access requests.

A record of all requests is to be kept.

6.7 Data Portability

Any individual whose personal data the School is in control or possession of may request that the School transmits to another organisation the applicable data about the individual specified in the request. This is called a data porting request.

If the department receiving the data porting request feels that the request should be rejected, the request shall be directed to the DPO for evaluation. If the DPO decides to reject the data porting request, he shall notify the requesting individual of the rejection within the time limit prescribed by the PDPA.

6.8 Security Principle

Appropriate physical, technical and organizational measures should be taken against unauthorized or unlawful processing, use, modification or disclosure, accidental loss, or destruction of, or damage to, personal data. This applies regardless of whether the personal data is processed electronically or in paper form. When personal data is not properly safeguarded, it can cause serious reputational damage to the School and can compromise the safety and trust of individuals whose personal data is held by the School. It is imperative to have appropriate security measures to prevent the personal data held by the School from being compromised whether accidentally or deliberately.

Before introducing any new system, tool, process, or enhancements thereof, appropriate physical, technical and organizational measures to protect personal data must be defined and implemented and a data protection impact assessment undertaken.

Security measures in place must be reviewed continually in order to adapt to changing regulatory landscape, technical developments or any physical or organizational changes.

6.9 Transfer Limitation Principle

When personal data is transferred to a third-party recipient, care should be taken to ensure that the third party upholds the same standard of data protection that is comparable to that under the PDPA, including the same level of security measures in protecting the personal data. The third party recipient may be bound to the same standard of data protection by operation of the law of the country in which it operates, or by a legally enforceable contract which imposes the required standard of protection, including security measures, limitations on the third party's use and retention of the personal data being processed, as well as safe destruction of the personal data when the third party no longer has a legal or business reason to retain the data.

Where the third-party recipient does not have a contract of service with the School, or its contract of service does not include clauses which impose obligations on the third-party recipient to uphold the same standard of data protection as that provided under the PDPA, the School shall require the third-party recipient to sign the School's "Letter of Undertaking for Service Providers of Tanglin Trust School Ltd".

The School shall also ensure that a third-party intermediary complies with the transfer limitation obligation set out in this section. A data protection impact assessment must be carried out before a third-party intermediary is used to process personal data for the School.

Where transfer is made through the use of cloud technology, the following steps must be considered to ensure protection of the data in the cloud:

- Ensure data security measures and IT risk assessments have been conducted and reviewed by the IT teams;
- When necessary, explore data anonymization or masking solutions or encryption technologies and tools.

6.10 Data Breach Management

Address all security and personal data incidents according to the School's Data Breach Response Plan and notify the regulator and the affected individuals where required under the plan and under the law.

6.11 Accountability Principle

The School should demonstrate responsibility for the personal data in the School's possession or control and compliance with the law on personal data protection.

The School must develop and implement policies for data protection, communicate and inform staff and intermediaries about these policies and implement processes and practices that are necessary to meet the obligations under the law. The School needs to also make information about the School's data protection policies, practices, and complaints procedure available to the community.

A Data Protection Officer (DPO) shall at all times be appointed to be in charge of all data protection related matters and act as a contact point for external parties whom the School collects personal data from. The contact information of the appointed DPO shall be made available on the School's website.

7 Record Keeping and Disposal

All records of collection, processing, transfer and disposal of personal data, including that of students, potential students, their families, employees and potential employees, must be kept and maintained in

an organised manner so that they can be made available to the regulator in a timely fashion and to data subjects if access is requested by the data subject as allowed under the law.

Records of data breach incident investigations must be created and kept in accordance with the Data Breach Response Plan.

Personal data can be retained only as long as required for legal and business purposes and shall be disposed of properly when it is no longer required for these purposes. Each school or department responsible for the personal data shall determine the time period each category of personal data may be retained for, and be responsible for the proper disposal thereafter.

8 Training and Awareness

All Employees will receive general information on data protection laws, regulations and internal policies through awareness and training sessions or communications. New joiners should complete the training as soon as reasonably practicable after commencement of employment. Records of the trainings must be kept.

Intermediaries, acting on behalf of the School, are also to receive appropriate training. Records of the trainings must be kept.

9 Data breach incidents

Any incidents involving the unauthorized disclosure of or access to, or the accidental or unlawful destruction, loss, alteration of, personal data transmitted, stored, or otherwise processed by the School shall be dealt with in accordance with the Data Breach Response Plan.

10 Compliance Reporting

At each meeting of the Risk and Compliance Committee, the Risk and Compliance Director shall update the Committee on the School's data protection status, including the following:

- Any material changes in data privacy requirements from the previous meeting arising from changes in the law or regulations.
- A summary of the Data Protection risk assessments, including key findings and action plans arising therefrom.
- A description of any regulatory examinations or audits (external or internal) undertaken, including key findings.

11 National Identification Documents and Numbers

National Identification documents and numbers refer to the Singapore NRIC, FIN, passport, Work Permit and Birth Certificate (collectively "ID"). IDs are personal data.

The School shall not collect, use or disclose any IDs or take copies of IDs except in the circumstances set out in the table at Appendix 1.

Where IDs are collected as allowed under this Policy, the data shall be classified as sensitive data and treated and stored as such.

Appendix 1: Purposes for which ID's May be Collected

Purpose	School / Department	Authorising source
Enrolment of students	Admissions; School Offices	Private Education Regulations
Recruitment of staff or Contractors providing service	HR / CCA / Operations	Employment Act; Private Education Regulations
Verification of Visitor identity	Operations (Security)	ADVISORY GUIDELINES ON THE PERSONAL DATA PROTECTION ACT FOR NRIC AND OTHER NATIONAL IDENTIFICATION NUMBERS Issued 31 August 2018
Examinations	Schools	ADVISORY GUIDELINES ON THE PERSONAL DATA PROTECTION ACT FOR NRIC AND OTHER NATIONAL IDENTIFICATION NUMBERS Issued 31 August 2018
Trips	Outdoor Education	[*passport details for travel*] ADVISORY GUIDELINES ON THE PERSONAL DATA PROTECTION ACT FOR NRIC AND OTHER NATIONAL IDENTIFICATION NUMBERS Issued 31 August 2018
Board of Governors	Corporate Secretariat	ACRA, Private Education Regulations