# NIS Data Privacy Policy and Notice

**Rationale:** The purpose of this document is to establish processes and protocols to ensure NIS abides by the best practices and principles laid out in the Amended Act on the Protection of Personal Information (APPI) (Personal Information Protection Commission, Japan), GDPR (General Data Protection Regulation) and any other applicable laws, regulations, or guidelines related to Data Privacy.

**Scope:** This policy applies to all parents, alumni, employees, suppliers and other users of NIS service

**Relationship to the mission:** At NIS, we acknowledge the importance of data protection and recognise that individuals have rights under the law in respect to the personal data we handle.

**Responsible Party:** The Data Protection Officer is responsible for administering and reviewing this policy.

**Definitions:**
For the purposes of this policy, the following terms apply:

- **Business Operator Handling Personal Information or Business Operator** means any organisation responsible for the proper handling of all Personal Information**.**

- **Individual Identification Code** means one prescribed by Cabinet Order which consists of any character, letter, number, symbol or other codes falling under any of the following items:
    - those able to identify a specific individual such as a character, letter, number or symbol into which a body feature of the individual has been converted in order to be processed by computers;
    - those characters, letters, numbers or symbols assigned which are stated or electromagnetically recorded in a card or other document issued to be able to identify a specific user, purchaser or recipient of products, services and benefits.

- **Data Controller** means the organisation which determines the purposes for processing Personal Data and the manner in which that processing will be carried out. In most cases, Nagoya International School will be the Data Controller of the Personal Data it collects and uses as part of its operational activities.

- **Data Processor** means the organisation or person that processes Personal Data on our behalf and in accordance with our instructions, such as suppliers and contractors. Our staff members are not Data Processors.

- **Data subjects or Principal** are all living individuals about whom we hold Personal Data.

- **Personal Data or Personal Information** means any information relating to a living individual who can be easily identified from that information or from any other information we may hold. Personal Data can include names, identification numbers, addresses (including IP addresses), dates of birth, financial or salary details, education background, job titles and images. Personal Data may be held on paper, in a computer or any other media whether it is owned by the

organisation or a personal device or other identifier or the equivalent, meaning all items (excluding individual identification codes) made by writing, recording, sound or motion, or other means, in a document, drawing, or electronic or magnetic record, this includes a record created in electronic or magnetic form (meaning electronic form, magnetic form, or any other form that cannot be perceived with the human senses); the same applies in items which can be used to identify a specific individual (this includes any information that can be easily collated with other information and thereby used to identify that specific individual).

- **Special care-required Personal Information or Sensitive Personal Data** means Personal Information comprising a principal's race, creed, social status, medical history, criminal record, information about being victim of a crime and other documents which handling require special care so as not to cause unfair discrimination, prejudice or other disadvantages to the Principal.
- **Personal Information Handling or Processing** means any activity which is performed on Personal Data or Special Category Data. It includes the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction of data.

## Key measures:

### Collection and retention of personal information

During the course of our operational activities, we will collect, store and process personal data, including information about children. We will endeavour to treat this data in accordance with legal safeguards and in a manner consistent with the high standards individuals have come to expect from our organization.

All our staff members are required to comply with this Data Protection Policy when processing Personal Data as part of their role. Failure to comply with this policy may lead to disciplinary actions in accordance with established policy.

We collect information from prospective employees and students during application processes. We collect personal information from alumni and donors, and from organizations who work with NIS or who employ our community members. This information is collected electronically and on paper forms and stored in various electronic databases.

We retain information on our students and their families, our alumni and employees for as long as it is relevant for the purposes of school operations. We delete information that is no longer needed (such as data stored about former prospective students or their families) Any time we begin collecting personal information from a new data subject, we will provide notice to, and or seek consent from the identifiable person or their guardian.

We store your personal data only to the extent and for as long as necessary to fulfill the purposes described in this Privacy Notice or to comply with legal obligations. In the interest of the integrity and confidentiality of personal data, we take appropriate technical and organizational measures. In particular, we implement physical and logical access controls and procedures for the regular review, assessment and evaluation of the effectiveness of the measures in accordance with our risk assessment. It may be processed beyond the end of our relationship to establish, defend or exercise claims (during the applicable limitation period), meet legal or post-contractual obligations, including legal documentation requirements, and to safeguard other legitimate interests of NIS.

**Utilization of personal information**
The personal information we collect is used to operate the school and provide related services. We use information about student learning to make decisions that help each child reach their potential. We use the email addresses of our community members to send targeted messages conveying important information. We store and use the phone numbers of NIS parents and their emergency contacts to ensure that students are kept safe. We store a large amount of personal information, and we use it with care in ways that align with our mission.

**Provision of personal information**
NIS shares personal information only in ways that would be expected by any reasonable person who is a data subject within the context of Nagoya International School. We transmit information between databases so that personal information is kept up to date in a variety of systems with only a single point of entry. Those systems hold data on our behalf. We share report cards and transcripts with other institutions when requested to do so in ways that help our students transition to other schools or universities. We share appropriate and accurate personal information with trusted adults, such as teachers, bus drivers, trip chaperones, medical professionals, and coaches in order to conduct school operations and ensure safety.

Access to special care personal information, such as religious, racial or ethnic group membership data or medical history records, (as defined in Article 2.3 of the Amended Act on the Protection of Personal Information) or other information deemed sensitive (such as child protection records or similar) is restricted to the appropriate employees. By default, employees only have the most basic access to personal information databases. Higher levels of access are granted only as necessary based on the role of the employee.

Trusted adults who are not employees of the school, such as trip chaperones, coaches, or parent volunteers, may be given access to personal information on an as-needed basis. These trusted adults will be required to agree to the current NIS data usage procedures.

Personal information is not transmitted, revealed, or disclosed to third parties except in cases where information is urgently required to protect the life, physical body, or possessions of another person and in cases specified by Article 23, Section 1 of the APPI.

**With whom we share personal data**
NIS will not share, sell, trade, or transfer your personally identifiable information to outside parties. However, this does not include trusted third parties who assist us in delivering our teaching and learning or conducting our services and operations to our stakeholders, so long as those parties agree to keep this information confidential and show adequate compliance with APPI laws. By joining NIS, stakeholders agree to allow NIS to release limited needed personal information to deliver a seamless and effective educational experience. Note that NIS may also release your information when we believe it is appropriate to comply with the law, enforce our school policies, or protect the rights and safety of others or the school.

In order to achieve the purposes described in this policy, it may be necessary for us to disclose your personal data with other businesses or organizations. The categories of recipients are as follows:

- other schools- Such as colleges/Universities and other pre-baccleaureate educational institutions educational institutions
- external service providers
- suppliers and other business partners
- authorities and courts
- Parents' Association as needed (contact details, main language spoken at home, and nationality, where you may object to such sharing of personal data)
- schools, colleges or universities that the students attend after leaving NIS

- other schools (amongst others for the purposes of trips, sports and activities)
- family nurses or doctors (amongst others where sharing is in the vital interests, or where not sharing could have a negative impact on the individual)
- tuition fee sponsors
- payroll providers, recruitment services provider, providers of IT hosting and maintenance services, providers of information systems that are necessary for NIS to deliver the admissions, administration, teaching and learning, pastoral development, and child protection services

We share student personal data to either enhance the student experience or improve school operations. All data sharing is done in line with legal requirements, through which we ensure that all personal data is securely processed by the third parties. In such cases, the third party is obligated to use that personal data in accordance with the terms of this privacy statement and APPI requirements. We will only transfer Personal Data to a Data Processor where they have provided us with sufficient guarantees that they will protect the data in compliance with data protection legislation and in line with our expectations. We will also ensure that these requirements are governed by contract or other legally binding agreement and will enter into Data Sharing Agreements with other Data Controllers, where this is considered appropriate.

We may disclose your personal data without your permission to the extent that it is required to do so by law in connection with any legal proceedings or prospective legal proceedings, and in order to establish, exercise or defend our legal rights.

We will not sell, distribute or lease your personal data to third parties unless we have your permission or are required by law to do so.

Transfers of personal data may occur to countries outside of Japan. If external recipients or external service providers are located in countries whose legislation does not guarantee an adequate level of data protection, NIS will implement suitable safeguards in the form of appropriate contractual clauses, namely standard contractual clauses and model contracts for data transfers recognized by the APPI, in order to ensure compliance with this Policy and applicable laws.

**Technical safety management and security of hard copy personal information**

NIS takes necessary and appropriate measures for security control of personal data. NIS uses encryption technology known as SSL (Secure Sockets Layer) on pages where users enter their personal information. SSL encrypts and authenticates information transmitted between the browser and the web server, preventing the theft or alteration of data by a third party.

NIS uses best practices in network security, including enforcement of strong passwords. We provide specific training to prevent targeted cyber-attacks. We abide by our legal obligations to report any data breach to the affected data subject(s) and the Personal Privacy Commission.

NIS keeps personal information that is in hard copy securely. Low-level personal information (such as student work which may be held by teachers for marking) should be kept within the appropriate learning environment (e.g. classroom, teacher workroom) but does not need to be in a secure location. Sensitive personal information (such as student records and personnel records and family records) should be retained inside locked offices and locked cabinets. Records that are deemed highly sensitive information (e.g. child protection records) should not be stored in the same location as other records and will always be kept in a locked cabinet within a secure room.

**Place of processing**

We process your personal data primarily within Japan. In order to achieve some of the purposes described above, it may also be necessary for us to process your personal data in countries outside Japan or to transfer

it to other countries. We process your personal data in or transfer the data to countries without adequate data protection on the basis of standard data protection clauses or legal exceptions (necessity for performance of a contract). NIS Website Data processing, please view the Privacy Policy located on our site www.nis.ac.jp.

**Data Subject Rights**

We recognise that Data Subjects have a number of rights regarding our use of their Personal Data, some of which are subject to conditions. All requests will be dealt with by our Data Protection Officer or our Data Protection Lead in accordance with our Information Rights Policy.

- **Right of access (commonly referred to as a subject access request)**
  This gives individuals the right to ask us about the Personal Data we use about them. This can include what we use it for, who we share it with, how long we store it and where we have obtained it from. Individuals can also ask for a copy of their personal data.
- **Right to rectification**
  This gives individuals the right to ask for inaccurate Personal Data to be corrected or for incomplete Personal Data to be completed.
- **Right to erasure ('right to be forgotten')**
  This gives individuals the right to ask for their Personal Data to be erased but the obligation for us to erase Personal Data only applies in certain circumstances.
- **Right to object**
  This gives individuals the right to ask us not to use their Personal Data. This will include the use of their data for direct marketing, or where automated decisions have been made about them.
- **Rights in relation to automated individual decision-making, including profiling**
  This gives individuals the right to object to decisions being made about them solely by automated means (without any human involvement) and to profiling (where automated processing is used to evaluate certain things about the individual).

If we are unable to comply with a request, then we will clearly inform Data Subjects about the reasons why.

**Policy Review**

This policy will be reviewed and confirmed as needed by the administration. The policy was originally drafted in April 2022. The most recent update and date of confirmation was March 2024.