DATA PROTECTION PRIVACY
DRAFT DOCUMENT

Updated May 2021

Pending Approval by the Board
Issue Date: May 2021

Table of Contents

Purpose of the AISA Data Protection :

These guidelines and procedures define how the American International School of Abuja (AISA) obtains, collects, uses, processes, secures, and protects **personal data** relating to individuals. It outlines the standards that must be adhered to and detail the Guidelines/procedures in place to ensure compliance with data protection laws.

This guidelines seek to ensure the school:

1. Sets clear standards on how personal data will be processed
2. Sets clear expectations for those who process data on behalf of the school
3. Evidence compliance with data protection standards and where applicable, and accreditation standards
4. Protects its reputation by processing personal data in line with the expectations of data subjects
5. Minimizes the risks of incidents relating to personal data

Personal data gathered by the school may include but is not limited to: individuals' phone numbers, email addresses, IP addresses, educational background, financial and salary details, details of certificates and diplomas, education and skills, marital status, nationality, job title, family make-up, dependents, next of kin, health information, gender, and images.

The school may also process 'sensitive categories' of data relating to data subjects, including information about an individual's racial or ethnic origin, political opinions,

religious or similar beliefs, trade union membership, physical or mental health or condition, criminal offences (or related proceedings) and genetic and biometric information.

National Information Technology Development Agency (NITDA)

In accordance with the Nigerian Data Protection Regulation (NDPR) AISA will adhere to and comply with all litigation set forth by the National Informational Technology Development Agency (NITDA) in order to protect the interests of our data subjects and follow the laws set forth by the Nigerian government. These bylaws will guide the AISA professional practice of data collection and data processing for all AISA. This document will also serve as a reference point for data subjects and their rights under the NDPR litigation.

The National Information Technology Development Agency (NITDA, hereinafter referred to as the Agency) is statutorily mandated by the NITDA Act of 2007 to, inter alia: develop Regulations for electronic governance and monitor the use of electronic data interchange and other forms of electronic communication transactions as an alternative to paper-based methods in government, commerce, education, the private and public sectors, labour and other fields, where the use of electronic communication may improve the exchange of data and information.

Governance

The American International School of Abuja is committed to complying with the laws of NITDA and NDPR. Therefore, all employees of AISA will follow the bylaws set forth by AISA that run compliant with NDPR. All decisions of action will come from the superintendent or administrative team. This includes but is not limited to data breaches, data collection purposes, communication with Nigerian authorities, etc. The Data Protection Officer (DPO) will consult on all data matters and give an outlined report or set of notes based on decisions made etc.

Accountability

The school will be accountable for demonstrating compliance with the key data protection principles. This will be performed by:

- Defining responsibilities for data processing activities within the school, • Training all members of staff, contractors, board members/governors on their data protection responsibilities,
- Appointing someone in the highest level of management to ensure the school has the appropriate resources to support compliance,
- Appointing a dedicated team to objectively oversee the school's compliance in the areas of data protection and cybersecurity,
- Undertaking regular independent and objective auditing of the school's compliance with data protection standards and ensuring the effectiveness of our organizational and technical measures for securing personal data,
- Facilitating a culture of data protection within the school by raising awareness of our data protection Guidelines, processes, and procedures, conducting Data Protection Impact Assessments (DPIA) where the school considers it necessary.

Data Protection Officer (DPO)

The Data Protection Officer is a position assigned by the superintendent to oversee school operations in regards to how data is being processed at the school. This DPO will serve the AISA community in a number of ways. The primary functions of the DPO are to:

- Inform and advise AISA and its staff of their data protection obligations under the NDPR
- Monitor the organization's compliance with the NDPR and internal data protection Guidelines and procedures. Includes monitoring the assignment of responsibilities, awareness training, and training of staff involved in processing operations and related audits. Data protection impact assessments (DPIAs), the manner of their implementation, and outcomes.

Data Protection	• Serve as a contact point to the data protection authorities including data breach reporting. • Serve as a contact point for individuals (data subjects) on privacy matters, including subject access requests. • Managing incidents involving data protection or cybersecurity • Managing requests from data subjects. Data protection is of the utmost importance. The school will act as the data controller for all data. The school controls the processing of personal data and the manner in which that data is processed. The school makes all decisions about how personal data is collected, used, stored, transferred, and kept secure. All staff should ensure: • All personal data is kept secure. • Personal data is not disclosed, accidentally or otherwise, to any third party. • Any new processing activity is evaluated using the school's DPIA procedure. • Ensuring any third-party processors engaged to comply with NITDA's standards of data protection. All data protection incidents are reported to the school's Data Protection Officer. • Any requests from data subjects involving access or amendments to personal data are referred to the school's Data Protection Officer. The school may require third parties to process personal data on their behalf. The school is committed to only use data processors who can comply with the NITDA standards. The school will publish these guidelines and procedures annually for staff, parents/guardians, and students. It is recommended that Parents/guardians and students familiarise themselves with this and privacy notice(s) as published. Guardians are expected to provide accurate and up-to-date data to the school. If a data breach incident has occurred affecting their personal data, they are encouraged to inform the school without delay. This data protection covers all personal data/sensitive category data processed by the school, on any school-owned or personal device. All staff, students, parents, contractors, and peripatetic staff are bound by this . Failure to comply with the may lead to disciplinary action. Each school, department, year group or stage, or departmental leader/manager is responsible for ensuring compliance with this in their respective area of responsibility.
AISA NITDA Compliant Guidelines	**Objective:** In order to best serve the AISA community, it is essential that certain data is collected. Different data may be collected by different departments for essential function-based reasons. Regardless of the department, AISA will keep all data secure and minimalized. AISA will also take special precautions when handling sensitive and or vulnerable data. **Data Collection:** This is a general breakdown of each department at AISA and the types of data being collected by each. It also includes a purpose or justification for needing the data for each:

Department	Types of Data Collected & Purpose
Human Resources	Data Type: *Name, address, email, sex, phone number of employee, emergency contact, nationality, educational background, employment history, email address, photograph, referee details.* Purpose: *Will be used for the identification, enrollment, and safety of the student*
Admission	Data Type: *Name, address, sex, email, employment*

	details of parents/guardians (name, phone number, residential and email address), photographs, educational background for change of school. Purpose: *Will be used for the identification, enrollment, and safety of the student*
Teacher (all divisions)	Data Type: *Attendance, grade reporting, language, behavior, individualized educational needs reporting.* Purpose: *Will be used for the safety, learning, and support of the student.*
Athletics	Data Type: *Name, grade, sex, passport, and contact information.* Purpose: *Will be used for the participation, safety, and logistics of a student.*
Security	Data Type: *Name, address, phone number, educational history, emergency contact, referee details, CCTV footage.* Purpose: *Will be used for the safety of the student.*
Advancement	Data Type: *Media (photographs, sound clips, videos)* Purpose: *Will be used for marketing purposes, or possibly emails for alumni functions.*
IT	Data Type: *School Email account and documents hosted via Google. Our cloud-based systems, etc.* Purpose: *Will be used for learning purposes.*
Finance	Data Type: *Payment/billing information, banking information, photograph, email address, financials (for staff)* Purpose: *Will be used for legal, financial, and procurement reasons.*

Administrative, Counselor. & Management	Data Type: *Name, grade, phone numbers, emails, incident, IEP, behavior reports, communications with constituents.* Purpose: *Will be used for the safety, learning, and*

	support of the student.
Nurse / Medical	Data Type: *Name, grade, sex, allergies, medical Incidents, medication.* Purpose: *Will be used for the safety and betterment of the student.*
Travel Logistics	Data Type: *Passport information (ID number, name, expiration dates, etc.)* Purpose: *Will be used to ensure students are able to travel to event destinations and find accommodations, etc.*

Erasure & Legacy:

Data will not be held for longer than necessary. Here is a breakdown of how long we will hold on to the different types of data based on use. Once the expiry date is met, that data will be erased from our servers.

Types of Data	Erasure (after leaving school or use)
Medical Records, CCTV footage, Logistics & Athletics Data	Up to 1 year
Google account, documents, email, etc. Media collected by advancement,	Less than 3 years
Class photographs, IEP Data, Behavior data, HR Data,	Less than 10 years
Financial records, alumni email records,	20 years
Personal Records (academic transcript, attendance, etc.)	Less than 100 years

Consent:

As a member of the AISA community, you will be asked to give the school your personal data. You will be given the option of saying yes or no to giving us your data. Below is a list of our consent guidelines:

	Guidelines
What is consent?	any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

When must we have consent?	- When there is no other lawful/legal basis - When using special category data (sensitive data)
How will we ask for consent?	- We will keep our consent request separate from general terms and conditions, and clearly direct people's attention to it; - use clear, straightforward, and easy to understand language; - avoid technical or legal jargon and confusing terminology (eg double negatives); - use consistent language and methods across multiple consent options; and - keep our consent requests concise and specific.
What will a consent request include?	- the name of our organisation and the names of any other controllers who will rely on the consent – consent for categories of third-party controllers will not be specific enough; - why we want the data (the purposes of the processing); - what we will do with the data (the processing activities); and - A place where people can withdraw their consent at any time.
What departments require consent?	Admissions/Registrar, Human Resources, Finance, IT, Teachers, Security, Advancement, Admin & Management, Logistics, and Medical.
How we will record consent	• **Who consented:** the name of the individual, or other identifiers. • **When they consented:** a copy of a dated document or online records that include a

	timestamp; or, for oral consent, a note of the time and date which was made at the time of the conversation. • **What they were told at the time:** a master copy of the document or data capture form containing the consent statement in use at that time, along with any separate privacy or other privacy information, including version numbers and dates matching the date consent was given. If consent was given orally, your records should include a copy of the script used at that time. • **How they consented:** for written consent, a copy of the relevant document, or data capture form. If consent was given online, your records should include the data submitted as well as a timestamp to link it to the relevant version of the data capture form. If consent was given orally, you should keep a note of this made at the time of the conversation - it doesn't need to be a full record of the conversation. • **Whether they have withdrawn consent**: and if so, when.
Withdrawing consent	You, the data subject, shall have the right to withdraw your consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, you, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent
How long does consent last?	Consent will be taken on an annual basis.
When is consent invalid?	- If we have any doubts over whether you have consented; - the individual doesn't realize they have consented; - we don't have clear records to demonstrate they consented; - there was no genuine free choice over whether to opt-in; - If you, the individual, would be penalized for refusing consent; - there is a clear imbalance of power between the school and the individual;

	- consent was a precondition of a service, but the processing is not necessary for that service; - the consent was bundled up with other terms and conditions; - the consent request was vague or unclear; - you use pre-ticked opt-in boxes or other methods of default consent; - AISA was not specifically named; - If we did not tell people about their right to withdraw consent; - If people cannot easily withdraw consent; or - the purposes or activities have evolved beyond the original consent.

Parental consent	The Nigerian Child Act Right 2003 states that a minor is a person under the age of 18 years. Hence, parental consent is advised for processing the personal data of children under the age of 18 years.

Vulnerable Data Subject:

A vulnerable data subject is anyone who is considered a minor. As nearly all of our students are minors their data needs to be even more thoroughly protected. Therefore, any time there is a need to gather data from vulnerable data subjects, the AISA DPO will assess if a data protection impact assessment (DPIA) is necessary and when one should be completed to ensure the security of said data.

Sensitive Data:

All sensitive data collected by AISA will only be done so with the explicit consent of the data subject or guardian. Categories of sensitive data are: Racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sexual orientation. Such information will not be shared without additional explicit consent from the data subject or guardian.

Data Collection

AISA's collection of personal data is of the utmost importance to us. This includes both electronic and paper data that we store. It is the responsibility of the school to ensure that all data is kept secured at all times. This is particularly true against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored, or otherwise processed. Such measures will include:

- Storing paper records securely, such as in a locked room, cupboard or desk. • Shredding paper records or disposing of them in a secure confidential waste bin for secure disposal, when no longer required.
- Encrypting and password protecting all school-owned devices.
- Encrypting and password protecting all school accounts in the cloud.

Security:

To ensure this security, AISA will follow the latest best practice Guidelines set by authorized regulators. Examples of our practice: only authorized personnel will have access to particular data sets. All data hosting will be secured through password protection and or physical locks, etc. For data breach information, find that section below.

The school will require all data subjects using its network to comply with its acceptable use and any other security or cybersecurity Guidelines as published from time to time.

The school will ensure that any transfer of personal data to third-party processors takes place only when the school is satisfied that the third party has appropriate technical and organisational measures in place to secure and protect the personal data

Travel:

At AISA students and staff travel and participate in a number of extracurricular events and training. These events range from traveling to foreign countries, sleeping in hotels,

Data Subject Rights	and taking flights. In order for students to participate, community members must consent to give the school their personal data that will be used for these purposes. It is the responsibility of the school to ensure the data processors (hotels, airlines, etc.) are in compliance with GDPR guidelines to ensure the protection of our students and staff data. Parents and staff will need to weigh the risk/reward of consenting to give this data if it is found that the processor is not GDPR compliant or certified. Data Sharing Partners: AISA will follow the Guidelines set in place by the NDPR in regard to the sharing of personal data with third parties. This data **will not** be shared without legal standing. Some examples of whom we may share this data are as follows: ● Universities and Other Educational Institutions ● The Nigerian Authorities ● Medical Hospitals or Clinics ● Cloud-based systems that we use for our day-to-day operations The school may transfer personal data to organisations outside Nigeria where it is necessary to aid cooperation between schools, where the transfer of student/family data between schools is required, where the transfer of staff data for the purpose of employment is required and where it is necessary for the delivery of our education and academic services (e.g sports trips, academic visits). The school is committed to only transfer data outside of Nigeria when one of the following circumstances occur:
Data Protection Impact Assessments (DPIA)	a) A transfer of personal data to a foreign country or an international organisation may take place where the NDPR has decided that the foreign country, territory or one or more specified sectors within that foreign country, or the international organisation in question ensures an adequate level of protection. b) The Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the Data Subject due to the absence of an adequacy decision and appropriate safeguards and that there are no alternatives. c) The transfer is necessary for the performance or conclusion of a contract between the Data Subject and the Controller or the implementation of pre-contractual measures taken at the Data Subject's request. d) The transfer is necessary for important reasons of public interest. e) The transfer is necessary in order to protect the vital interests of the Data Subject or of other persons, where the data subject is physically or legally incapable of giving consent At AISA we ensure that all of our data subjects know their rights and that we are protecting them in accordance with the law:
Data Processor Evaluation	● A data subject is a natural person who is not fictitious or deceased. ● Data subjects have the right to information relating the processing (both where data is obtained by first and third parties) ● Data subjects have a right to access their data upon request ● Data subjects have a right to rectification, erasure, and restriction of processing ● Data subjects have the right of portability (request for data to be transferred to another processor) ● Data subjects have the right to object from giving their data ● Data subjects have the right to ask for their data to be transported to another institution. Upon request, AISA will transport this data in a format that is universally accepted. This data will be transported in a timely manner and will not exceed one school calendar year. The school will consider the risks to data subjects when processing personal data and will put in place proportionate organisational and technical measures to ensure a level of protection appropriate to those risks.

Data Breach Protocols	Where processing is deemed to be high risk, the school will complete a DPIA in order to evaluate that risk and put in place any measures deemed necessary to mitigate it. The school will complete a DPIA in the following circumstances:- 1. Where new technology is intended to be used (such as new applications, systems or infrastructure). 2. Where existing technology is being changed or upgraded. 3. Where decisions are being made about individuals as a result of automated processing or profiling Where processing of sensitive category data is intended to take place on a large scale. 4. Where imaging systems are intended to be used in a way that may raise privacy concerns. The school has a template for the completion of DPIA's which can be obtained from the Data Protection Officer.
Exercising Your Data Privacy Rights at AISA	For all data that is held at the American International School of Abuja, a thorough data processor evaluation will take place to ensure the security of the data and compliance of the company. This data processing evaluation will be done by the DPO and will happen BEFORE a new system is agreed upon for use or data is actually collected. The DPO will look to ensure the data processors of school data are either GDPR certified, have a GDPR adequacy decision in place, have a BCR in place, or include standard contract clauses in place to protect our data.
The Use of Personal Social Media Accounts	The school has procedures in place to manage incidents relating to personal data. Everyone is responsible for reporting actual or suspected incidents involving personal data. This includes IT and cybersecurity incidents. All incidents must be reported to the DPO without delay, by emailing dpo@AISAagos.org including (where possible) the following information: ● Name of individual reporting, and contact details ● Date and time of the incident ● Details of the incident ● Type of data affected e.g. names, medical information ● Number of individuals affected (if known) Disciplinary action may be taken against individuals who do not report incidents If there is any mention or fear of a data breach at AISA, an investigation will begin immediately by the DPO and IT team to confirm or disconfirm it. If there ever is a time in which there is a confirmed data breach, AISA affected community members will be notified of the said breach without undue delay. This notification will include a breakdown of what data was breached, how it was breached, how it can possibly expose a staff member further, and what preventative measures can be done in the meantime. A final report will be made by the DPO to give a breakdown of the event, where security failed, and a plan or suggestion of what improvements will need to be set in place for the future.
GDPR Glossary & Definitions	All people under the Nigerian data protection law have data subject rights (see above). These rights apply to all members of our community and AISA will honor them fully. If for any reason you feel your rights are not being honored or respected or there has been a violation of your rights by AISA, you have the right to contact the NITDA to form an official complaint.

Personal social media means individual personal accounts of Facebook, Instagram, WhatsApp, LinkedIn, Dropbox or variations thereof. The use of personal social media accounts for school business purposes has implications on the school's ability to comply with data protection law. The school cannot adequately protect personal data or support

Data subjects if invoking their information rights if their personal data is held in the personal social media accounts of school staff, peripatetic staff, volunteers or governors/board members. The subsequent processing of personal data by social media companies has significant privacy risks for all data subjects.

For these reasons, the use of personal social media accounts for the processing of personal data collected by the school is forbidden. Where lawful, personal data will be used in corporate/school-owned and managed social media accounts. Further information on the school's for social media can be found here

DPO - Data protection officer. Responsible for advising the organization and its employees of their data protection obligations under the GDPR. Monitor the organization's compliance with the GDPR. Serve as the contact point between authorities and individuals on privacy matters.

Personal Data - Any information relating to a person (data subject) who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of a person.

Processor - Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Sub Processor - a hired entity or person who assists processors in the processing or storage of data.

Controller - The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Joint Controllers - Where two or more controllers jointly determine the purposes and means of processing.

Data Subject - An Identified or Identifiable living individual to whom personal data relates. In the context of this , data subject shall mean prospective staff and students, current staff and students, parents and guardians of prospective and current students, peripatetic staff, former staff, alumni, members, contractors, visitors, website visitors and school contacts.

DPIA - Data protection impact assessment is a process in which the DPO verifies the security and validity of a new data collection measure or tool.

Sensitive Data - Racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sexual orientation

Vulnerable Data Subject - children, employees, mentally ill persons, asylum seekers, or the elderly, patients, and where there is an imbalance in the relationship between the position of the data subject and the controller.

GDPR - General Data Protection Regulation. A set of laws set in place to protect the

personal data of all people under its governance. These laws are enforced by the authorities that created these laws.

Consent - is the permission given to another to allow for something to happen that was requested. Consent is valid when it is freely given, specific to what is being asked, the consenter is fully informed, it is unambiguous, and is of the appropriate age consent.

Adequacy Decision - an agreement and verification by the EU and another country that allows for data to flow freely between the two parties because data protection laws are being met.

Binding Corporate Rule (BCR) - Binding Corporate Rules or "BCRs" were developed by the European Union Article 29 Working Party to allow multinational corporations, international organizations, and groups of companies to make intra-organizational transfers of personal data across borders in compliance with EU Data Protection Law.

Derogation - When explicit consent is given to transfer data in a non-repetitive manner for a limited number of data subjects.

Privacy Shield - A compliance certification given by the EU to US companies that have proven GDPR compliance and regulation.

Legitimate Interest - Processing data is **necessary** for the purpose of the legitimate interest pursued by the controller or by the third party or parties to whom the data is disclosed

Public Interest - Processing data is **necessary** for the performance of a task carried out in the exercise of official authority vested in the controller

Vital Interest - Processing data is **necessary** to protect the data subject's life

Legal Obligation - Processing data is **necessary** for you to comply with the law (not including contractual obligations).

Contractual necessity - Processing data is **necessary** for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into the contract.

Personal data: any information relating to an identified or identifiable individual ('data subject'). An identifiable individual is one who can be identified, directly or indirectly by an identifier, such as a name, an identification number, a location, an online identifier or by one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.

Data subjects: in the context of this mean prospective staff and students, current staff and students, parents and guardians of prospective and current students, peripatetic staff, former staff, alumni, members, contractors, visitors, website visitors and school contacts.

Processing: means any operation or set of operations which is performed on personal data/sensitive category data or on sets of personal data / sensitive category data, whether or not by automated means, such as; collecting, recording, organising, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, restricting, erasing or destroying data.