LIFEFORTE INTERNATIONAL SCHOOLS
DATA PROTECTION POLICY
2025/2026 Session

Purpose of this Policy
This document outlines the Data Protection Policy for Lifeforte International Schools. Within the meaning of Section 65 of the Nigeria Data Protection Act 2023, Lifeforte International Schools is a Data Controller.

Introduction
For the purposes of but not limited to education, training and employment, the school collects and uses certain types of personal information about students, parents/carers, staff and other individuals who come into contact with it.
This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the Nigeria Data Protection Act 2023 and other related legislation. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Data Protection Regulation
There are 6 personal data processing principles as laid down in the 2023 Data Protection Act which must be followed at all times, unless an exemption applies:

Transparency
Data must be processed in a fair, lawful and transparent manner.

Purpose and limitation
Data must be collected for specified, explicit, and legitimate purposes, and not to be further processed in a way incompatible with these purposes. A data controller has an obligation to specify in its privacy policy the purpose of processing personal data and provide the data subject prior to processing for any further purpose information on that other purpose.

Limitation
The data processing must be adequate, relevant, and limited to the minimum necessary for the purposes for which the personal data was collected or further processed
Accuracy
Personal data processed must be accurate, complete, not misleading, and, where necessary, kept up to date having regard to the purposes for which the personal data is collected. A data subject has the right to access and rectify their data

Storage Limitation
Personal data collected must not be retained for longer than is necessary to achieve the lawful bases for which the personal data was collected or further processed. A data controller has to stipulate in its privacy policy the period for which personal data will be stored, or if that is not possible, the criteria used to determine that period

Confidentiality
Data must be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing, access, loss, destruction, damage, or any form of data breach. A data controller is required to put in place data security apparatus so as to keep the collected data confidential and protect it against attacks

Policy Statement

The School is committed to maintaining the 6 principles outlined above. This means that the school will:

- Obtain consent if required for the processing of personal data (please note that consent may not be required if the processing is necessary for the school to undertake its obligations to students, and their parents/carers).
- If information is shared we will (except in occasional circumstances where it is lawful and appropriate not to do so) explain to those concerned why, with whom and under what circumstances;
- We will check the quality and accuracy of the information we hold;
- Review the data we hold at regular intervals to ensure personal information is not held longer than is necessary;
- Ensure that when information is properly authorised for disposal this is done securely;
- Ensure appropriate security measures to safeguard personal information whether that is held in paper files or on our computer system;
- We will share personal information with others when it is necessary and legally appropriate to do so;
- Train our staff so that they are aware of our policies and procedures;
- This policy will be updated as necessary to reflect best practice or amendments made to the Data Protection Act 2023 and subsequent legislation, regulation or guidance

Sensitive personal data
The school may, from time to time, be required to process sensitive personal data about staff, students or parents. Sensitive personal data includes medical information and data relating to religion, race, criminal records and proceedings. Where sensitive personal data is processed by the School, the explicit consent of the subject will generally be required but there are circumstances where it is not: for example, where necessary to protect the vital interests of individuals, or where required by law (including in the context of employment) or by a statutory authority.

Data Protection at Lifeforte International Schools
Data Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the school of a change of circumstances we will update our records as soon as is practicable.
Where a data subject challenges the accuracy of their data, the school will immediately mark the record as potentially inaccurate and until resolved the marker will remain and all disclosures of the affected information will contain both versions of the information.

Data adequacy and relevance
Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the school will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

Authorised disclosures
The school will, in general, only disclose data about individuals with their consent. However there are circumstances under which the school may need to disclose personal data – even sensitive personal data – without explicit consent for that occasion. These circumstances are generally limited to:

- Student data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations;
- Student data disclosed to authorised recipients in respect of safeguarding (health, safety and welfare);
- Student data disclosed to parents/carers in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school;
- Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters; or where expressly requested by a relevant authority.

Only authorised and trained staff are allowed to make external disclosures of personal data and internal processing of personal data, in particular sensitive personal information, is handled by appropriate staff on a need-to-know basis. Data used within the school by administrative staff, teachers and those external agencies with which we work, will only be made available where the person requesting the information is a professional legitimately working within the school who needs to know the information in order to do their work.

The school will not disclose anything on students' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything which suggests that they are, or have been, either the subject of or at risk of child abuse. See **Safeguarding Policy** for further information.

Subject Access Request
Individuals have a right to make a 'subject access request' to request a copy of the personal information that we hold about them. Subject access requests must be submitted in writing. Requests should include:

- T he user's name;
- A correspondence address;
- A contact number and email address;
- Details about the information requested.

The school will not reveal the following information in response to subject access requests:

- Information that might cause serious harm to the physical or mental health of the user or another individual;
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests;
- Information contained in adoption and parental order records;
- Certain information given to a court in proceedings concerning the child.

Subject access requests for all or part of the student's educational record will be provided within 10 working days.

Data and computer security

Physical security

Appropriate building security measures are in place, such as window locks and deadlocks. Laptops and printouts are locked away securely when not in use. Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied whilst in the building.

Electronic data security

Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files that are password protected.

Procedural security

In order to be given authorised access to the computer network, staff will have to sign an Acceptable Use Policy (see ICT Policy). All staff are trained in their data protection obligations and their knowledge updated as necessary. Printouts as well as source documents containing confidential information are shredded before disposal. The school is liable as data controller for the acts of its staff, but individual members of staff should be aware they can be personally liable in law for security failures or wrongful disclosures including under the law of libel, confidentiality, or misuse of private information.

Disposal of Records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely. For example, we will shred or incinerate paper-based records, and override electronic files. We may also use an outside company to safely dispose of electronic records.

Training

Our staff members are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation or the School's processes make it necessary.

Complaints

Any complaints about this policy should be brought to the attention of the Head of School.
Complaints that are in the public interest and relate to suspected malpractice may be appropriate to raise under the school's Whistleblowing Policy.

Compliance and Performance Monitoring

The School will review this policy every two years and ensure that its practice is in line with this policy. Any review will take into account the most up-to-date legislation and guidance.

Explanation of Terms

School
Lifeforte International Schools

Personal data
Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified

Sensitive personal data
Data such as:

- Racial or ethnic origin
- Religious beliefs, or beliefs of a similar nature
- Physical and mental health
- Whether a person has committed, or is alleged to have committed,
- an offence
- Criminal convictions