Data Protection Policy

1. Introduction

The International Academy (the School) collects and uses information about various individuals to operate effectively. This includes information about:

- Members of the public
- Current, past, and prospective employees
- Clients and customers
- Suppliers
- Students (including their parents/guardians)

The School is committed to ensuring that personal data is managed properly and complies with current data protection legislation. We will make every effort to meet our obligations under the legislation and regularly review procedures to ensure compliance.

This policy applies to all staff (including temporary staff), contractors, agents, volunteers, and representatives working for or on behalf of the School. It covers all personal data created or held by the School, regardless of format (electronic, paper, email, etc.) and storage method (ICT systems, databases, filing cabinets, etc.).

2. Scope

Personal data is information about living individuals that can be used to identify them. This includes both factual and opinion-based data, and it can be part of a computer record or manual record.

3. Responsibilities

The Board of Directors has overall responsibility for ensuring the School meets the legal requirements of data protection legislation. The school’s principal has overall responsibility for information management.

The Principal is responsible for ensuring compliance with data protection legislation and this policy within the School's daily activities.

Contractors who collect or hold personal data on behalf of the School must comply with data protection legislation and ensure information is processed according to the School's instructions and this policy.

4. Data Protection Principles

Data protection legislation requires anyone processing personal data to comply with six legally enforceable principles:

1. **Fairness and Lawfulness:** Personal data must be processed fairly, lawfully, and transparently.
2. **Purpose Limitation:** Data must be collected for specified, lawful purposes and not further processed in a way incompatible with those purposes.
3. **Data Minimization:** Data must be adequate, relevant, and not excessive for the processing purpose.
4. **Accuracy:** Data must be accurate and kept up to date when necessary.
5. **Storage Limitation:** Data must not be kept longer than necessary for the processing purpose(s).
6. **Security:** Data must be protected by appropriate security measures.

The School is responsible for demonstrating compliance with these principles and ensuring data is processed in accordance with the rights of data subjects. Additionally, personal data must not be transferred to a country without an adequate level of data protection unless another secure method is guaranteed.

5. Privacy Notices

Whenever the School collects information about individuals, they will be informed of the following at the point of collection:

- The identity of the data controller (the School)
- Contact details of the Data Protection Officer
- The purpose for collecting the information
- Any other purposes for which it may be used
- The lawful basis for processing the data
- Who the information will be shared with
- Whether the data will be transferred outside Libya and, if so, how it will be kept secure
- How long the data will be kept
- How data subjects can exercise their rights

The School will review its Privacy Notice annually and alert students and parents to any updates.

6. Data Protection Officer

The School has appointed a Data Protection Officer to comply with data protection requirements.

7. Data Breaches

All staff (including temporary staff), contractors, agents, volunteers, and representatives must report a security incident or data breach to the Principal immediately, following the Data Breach Policy.

8. Consent

Where the School processes data with consent (e.g., publishing student photos or sending marketing emails about school uniforms), it will ensure the consent is freely given, specific, informed, and unambiguous, and that it is recorded.

9. Information Society Services

For Information Society Services (online services with a commercial element) targeted at children, the School will take reasonable steps to seek consent from the child's parent/guardian if the child is under 13.

10. Direct Marketing

The School will only send electronic direct marketing materials (emails, SMS texts, faxes, or recorded phone messages) if the recipient has given explicit consent (e.g., opted in by ticking a box).

11. Provision of Data

Disclosure of Personal Data

Relevant, confidential data should only be disclosed to authorised individuals or entities on a need-to-know basis. This includes:

- Other staff members who require the information to perform their duties.
- Relevant parents/guardians with parental responsibility for the student.
- Other authorities if it is necessary in the public interest, such as for:
    - Crime prevention
    - Safeguarding children
- Other authorities (e.g., Local Authority, new schools) with legitimate requirements for the information (e.g., transferring student records).

Safeguarding Pupil Information

The School should not disclose anything on a pupil's record that could potentially harm their physical or mental health or that of anyone else. Those creating such records should ensure this information is separated from other records.

Confidentiality and Parental Responsibility

- If there is doubt about who has parental responsibility or if statutory requirements conflict, legal advice should be sought.
- When there are safeguarding concerns, the matter should be referred to the School's Designated Safeguarding Leads (DSL).

- When providing information to an individual, particularly by telephone, verify their identity. Ask questions only the individual would likely know the answers to.
- Information should not be provided to other parties, even if related (e.g., divorced parents). Take care when there is any doubt about parental responsibility.

12. The Individual's Rights

Subject Access Requests

Anyone whose details are held by the School has the right to request a copy of the information held about them (or their child). They can also inquire about the accuracy of the data and who it is shared with.

The School must handle these requests promptly, providing a response within one month (or 15 school days for education records) upon receiving a request. All staff must recognize and log such requests immediately with the Principal.

13. Provision of Data to Children

Determining a Child's Capacity

The Information Commissioner's Office (ICO) provides guidance on a child's capacity to make a subject access request. Generally, by the age of 12, a child can be expected to have sufficient maturity to understand the nature of the request. However, a child may reach this maturity earlier, and each case should be judged individually.

- If a child does not understand the request, someone with parental responsibility (parent or guardian) can make the request on their behalf and receive a response.
- Pupils who submit requests to access their educational records should be allowed to do so unless it's clear they don't understand what they're asking for.

14. Parents' Rights

Parental Access to Student Information

An adult with parental responsibility can access information about their child, as long as the child is not considered mature enough to understand the request. They must be able to prove their parental responsibility. The School may request relevant documentation to verify this, along with the identities of the requestor and child.

15. Information Security

Safeguarding Personal Data

All staff members must be vigilant about protecting personal data from unauthorised access. This includes:

- **Computer Security:**
    - Don't leave computer screens visible to the public.
    - Use strong passwords and log out when not using a computer.

    - Don't store school data on removable devices (USB sticks, etc.) unless encrypted and password-protected.
    - Permission from the Principal is required to use personal devices for school purposes.
- **Physical Security:**
    - Securely store paper files containing personal data in locked cabinets when not in use.
    - Don't leave personal data unattended off-site (e.g., in a car overnight).
- **Email Security:**
    - Double-check email addresses and attachments before sending.
    - Use the BCC field for external recipients to avoid revealing everyone's email addresses.

16. Maintaining Up-to-Date Data

The School will only retain personal data for as long as necessary for legal or legitimate business purposes. This typically means keeping data for the duration of a student's enrollment at the School, plus an additional period determined by the School. Outdated or irrelevant data will be securely discarded.

17. Inaccurate Data

If an individual believes the data the School holds about them is inaccurate, incomplete, or wrong, they have the right to complain. The School will thoroughly investigate the complaint and respond within one month. In the meantime, a note will be added to the individual's file indicating the disputed information. Individuals also have the right to apply to the court for a correction order.

18. Data Recording

Records should be kept in a format that allows individuals to inspect them and could potentially be reviewed by legal authorities. This means ensuring data is:

- Accurate and unbiased
- Clear, unambiguous, and factual
- Easily readable and decipherable
- Documented with the source and date of acquisition (for information obtained externally).

Written consent is required before including any personal information (of an individual or their child) on the School's website, and individuals will be informed about the implications of their data being publicly available.

19. Photographs

The School takes student privacy seriously and seeks written parental permission before using photographs of students outside of the School setting. Parents can also opt-out of having their child's photograph taken altogether.

20. Breach of Policy

Non-compliance with data protection legislation by staff members is a serious offence and a disciplinary matter. Depending on the severity, it could lead to dismissal without notice. Additionally, individuals can commit a criminal offence by obtaining or disclosing personal data without authorization.

21. Review of the Policy

This policy will be reviewed every two years (bi-annually) to ensure it remains current and effective.

22. Glossary

Term	Definition
Data Controller	A data controller is the individual or the legal person who controls and is responsible for the keeping and use of personal information on computer or in structured manual files.
Data Subject	The individual who the data or information is about.
Educational record	The educational record is confined to information that comes from a teacher or other employee of a local authority or school, the pupil or their parents. Communications about a particular child from head teachers and teachers at a school and other employees at an education authority will therefore form part of that child's official educational record, as will correspondence from an educational psychologist engaged by the governing body under a contract of services. It may also include information from the child and their parents, such as information about the health of the child. Information kept by a teacher solely for their own use does not form part of the official educational record.
Information Commissioner	The independent regulator who has responsibility to see that the data protection legislation is complied with. They can give advice on data protection issues and can enforce measures against individuals or organisations who do not comply with the law.
Notified Purposes	The purposes for which the school is entitled to process that data under its notification with the Office of the Information Commissioner.
Personal Data	Defined as 'data which relates to a living individual who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller' or an identifier (the school is a data controller), and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other in respect of the individual.
Processing	Covers a broad range of activities such that virtually any use of personal information or data will amount to processing. Just holding or storing the data constitutes processing.
Processed fairly and lawfully	Data must be processed in accordance with the provisions of data protection legislation. These include the data protection principles, the rights of the individual and notification.
Special Category (sensitive) Data	Information about racial or ethnic origin, sexual life, religious beliefs (or similar), physical or mental health/condition, membership of a trade union, political opinions or beliefs, or biometric or genetic data.
Subject Access Request	An individual's request for personal data under the General Data Protection Regulation.