ليـــوا للتعليم
Liwa Education

Data Protection and Privacy Policy

Policy Document

2024-2025

August 2024

Policy Reference	ET-07-En
Version	V2
Policy Owner	IT Manager
Reviewed by	Director of Schools
	Deputy CEO
Approved by	CEO
Date of Creation (V1)	10102023
Review Date (V2)	01082024
Review Date (V3)	01082026
Effective Date (Latest Version)	01082024

Rationale

The school collects and uses personal information about staff, pupils, parents, and other individuals who come into contact with the school. This information is gathered to enable the school to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

The school ensures compliance with Federal Decree Law No. (45) of 2021 on the Protection of Personal Data. This law serves as the basis for our data protection practices, ensuring that personal information is handled lawfully, securely, and transparently.

Also, the UAE's constitution and federal laws i.e. Federal Law No. 5 of 1985: The Civil Code and the Federal Law No. 3 of 1987: The Penal Code ('the Penal Code') gives citizens a general right to privacy. The school will assume the role of the data controller. This means that the school is responsible for deciding the personal data collected and how this is stored. The policy explains the general principles that will be used in processing the data, what personal data will be used and how long it will be retained for. The policy will also outline the steps you can take if you feel that we have used your data incorrectly.

Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username

	It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data, which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purpose • Health – physical or mental
Processing	Anything done to personal data, such as collecting, recording, organizing, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organization that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.

The Data Controller

Liwa Schools processes personal data relating to parents, students, staff, Governors, visitors and others, and therefore is a data controller.

Roles and Responsibilities

This policy applies to **all staff** employed by Liwa Schools and to external organizations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Governing Body

Liwa Education Board of Trustees has overall responsibility for ensuring that Liwa Schools complies with all relevant data protection obligations. The key gatekeeper of this responsibility is the CEO.

Data Protection Officer (DPO)

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the Board of Trustees and, where relevant, report to them their advice and recommendations on Liwa Schools data protection issues.

The DPO is also the first point of contact for individuals whose data Liwa processes, and for the School Principal.

Full details of the DPO's responsibilities are set out in their job description. Our DPO is the Human Resource Officer.

School Principal

The School Principal acts as the representative of the data controller on a day-to-day basis.

All staff

Staff are responsible for:

1. Collecting, storing and processing any personal data in accordance with this policy.
2. Informing the school of any changes to their personal data, such as a change of address.

3. Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure. If they have any concerns that this policy is not being followed.
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way.
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UAE.
    - If there has been a data breach.
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
    - If they need help with any contracts or sharing personal data with third parties.

DATA PROTECTION PRINCIPLES

The Data Protection Law is based on data protection principles that our school must comply with. The principles say that personal data must be:

1. Processed in accordance with Article 10
2. Processed lawfully, fairly and in a transparent manner in relation to a Data Subject.
3. Processed for specified, explicit and legitimate purposes determined at the time of collection of Personal Data.
4. Processed in a way that is not incompatible with the purposes described in Article 9(1)(c); (e) relevant and limited to what is necessary in relation to the purposes described in Article 9(1)(c)
5. Processed in accordance with the application of Data Subject rights under this Law.
6. Accurate and, where necessary, kept up to date, including via erasure or rectification, without undue delay.
7. Kept in a form that permits identification of a Data Subject for no longer than is necessary for the purposes described in Article 9(1)(c)
8. Kept secure, including being protected against unauthorised or unlawful Processing (including transfers), and against accidental loss, destruction or

damage, using appropriate technical or organisational measures.

This policy sets out how the school aims to comply with these principles.

COLLECTING PERSONAL DATA

Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

1. The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract.
2. The data needs to be processed so that the school can **comply with a legal obligation.**
3. The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
4. The data needs to be processed so that the school, as a public authority, can perform a task
    - **in the public interest,** and carry out its official functions
5. The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden).
6. The individual (or their parent/carer when appropriate in the case of a student) has freely given clear **consent.**
7. For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the Data Protection Law 2020.
8. If we offer online services to students, such as classroom applications, and we intend to rely on consent as a basis for processing, we will get parental consent when the student is under 13 (except for online counselling and preventive services).
9. Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.
10. Individuals have the right to withdraw their consent for the processing of personal data at any time. When consent is withdrawn, the school will cease

processing the relevant data unless a legal basis exists to continue. Individuals will be informed of any such legal requirements.

Limitation, Minimisation and Accuracy

1. We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

2. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

3. Staff must only process personal data where it is necessary in order to do their jobs.

4. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymized. This will be done in accordance with the school's records and retention schedule.

Sharing Personal Data

We will not normally share personal data with anyone else, but may do so where:

1. There is an issue with a student or parent/carer that puts the safety of our staff at risk.
2. We need to liaise with other agencies – we will seek consent as necessary before doing this.
3. Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:
   - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
   - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
   - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us
4. Only appoint suppliers or contractors which can provide sufficient guarantees

that they comply with data protection law.

5. Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
6. Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.
7. We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:
    - The prevention or detection of crime and/or fraud
    - The apprehension or prosecution of offenders
    - In connection with legal proceedings
    - Where the disclosure is required to satisfy our safeguarding obligations
    - Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided
8. We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.
9. Where we transfer personal data to a country or territory outside of the UAE, we will do so in accordance with data protection law

SUBJECT ACCESS REQUESTS AND OTHER RIGHTS AND INDIVIDUALS

1. Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

1.1 Confirmation that their personal data is being processed
1.2 Access to a copy of the data
1.3 The purposes of the data processing
1.4 The categories of personal data concerned
1.5 Who the data has been, or will be, shared with
1.6 How long the data will be stored for, or if this isn't possible, the criteria used to determine this period1.7
1.7 The source of the data, if not the individual

1.8 Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email, or fax to the DPO. They should include:

- Name of Individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request, they must immediately forward it to the DPO.

2. Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our school may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

3. Responding to subject access requests

When responding to requests, we:

3.1 May ask the individual to provide 2 forms of identification
3.2 May contact the individual via phone to confirm the request was made
3.3 Will respond without delay and within 1 month of receipt of the request
3.4 Will provide the information free of charge
3.5 Respond within one month of the request being made, however, we may tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month and explain why the extension is

necessary.

We will not disclose information if it:

1. Might cause serious harm to the physical or mental health of the student or another individual
2. Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
3. Is contained in adoption or parental order records
4. Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why and tell them they have the right to complain to the School Principal.

4. Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

4.1 Withdraw their consent to processing at any time

4.2 Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)

4.3 Prevent use of their personal data for direct marketing

4.4 Challenge processing which has been justified on the basis of public interest

4.5 Request a copy of agreements under which their personal data is transferred outside of the European Economic Area

4.6 Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)

4.7 Prevent processing that is likely to cause damage or distress

4.8 Be notified of a data breach in certain circumstances

4.9 Make a complaint to the School Principal

4.10 Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

5. Parental requests to see the educational record

Parents, or those with parental responsibility, who would like to see their child's educational record (which includes most information about a student) must make a request in writing.

CCTV

1. We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

2. We do not need to ask individuals' permission to use CCTV. Security cameras are clearly visible. Only SLT can view CCTV footage to assist with any investigation.

3. Any enquiries about the CCTV system should be directed to the School Principal.

Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within Liwa Schools

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing, and promotional materials upon enrollment to the school.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Any photographs and videos taken by parents/ carers at the school for their own

personal use are not covered by data protection legislation. However, we will ask that photos or videos are not taken of other students unless express permission has been provided.

Uses may include:

- Within the school on notice boards and in the school prospectus/handbooks, display photos around the school, and the school newsletters.
- Outside of the school by external agencies such as the school photographer, newspapers, and campaigns.
- Online on our school website or social media pages.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Data Protection by Design and Default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

1. Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
2. Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law.
3. Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process).
4. Integrating data protection into internal documents including this policy, any related policies and privacy notices.
5. Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance.
6. Regularly conducting reviews and audits to test our privacy measures

and make sure we are compliant.

7. Maintaining records of our processing activities, including:
8. For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
9. For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

Data Security and Storage of Records

We will protect personal data and keep it safe from unauthorized or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

1. Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
2. Papers containing confidential personal data must not be left on office and classroom desks, on staff room tables, pinned to notice/display boards, or left anywhere else where there is general access
3. Passwords are used to access school computers, MacBook's and other electronic devices. Staff and students are reminded to change their passwords at regular intervals
4. Encryption software is used to protect all portable devices and removable media.
5. Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment.
6. Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred or incinerate paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Personal Data Breaches

The school will make all reasonable endeavors to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1. When appropriate, we will report the data breach to the School Principal within 24 hours. Such breaches in a school context may include, but are not limited to:

1. A non-anonymised dataset being published on the school website which shows the exam results of students
2. Safeguarding information being made available to an unauthorised person
3. The theft of a school device containing non-encrypted personal data about students

TRAINING

All staff and the Board of Trustees 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, guidance or the school's processes make it necessary.

MONITORING ARRANGEMENTS

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed and updated on an annual basis to ensure changes are reflected appropriately.

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

1. On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
2. The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
3. The DPO will alert the School Principal who will alert the Board of Trustees
4. The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
5. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
6. The DPO will work out whether the breach must be reported to the School Principal. This must be judged on a case-by-case basis.
7. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data Discrimination
    - Identifying theft or fraud Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned
    - If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the School Principal
8. The DPO will document the decision (either way), in case it is challenged at a later date by the School Principal or an individual affected by the breach. Documented decisions are stored on the

school's computer system.

9. Where the School Principal must be notified, the DPO will do this setting out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
10. If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
11. The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
12. The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
13. The DPO will document each breach, irrespective of whether it is reported to the Commissioner. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
    - Records of all breaches will be stored on the school's IT system.
    - The DPO and School Principal will meet to review what happened and how it can be stopped from happening again.

This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take appropriate actions to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

14. If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
15. Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
16. If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
17. In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
18. The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
19. The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Equality Impact Statement

The school will do all it can to ensure that this policy does not discriminate, directly or indirectly. It will ensure this through regular monitoring and evaluation of policies. On review the school will assess the likely impact of its policies on the promotion of race equality, equality for disabled persons, gender equality and cohesion.

Policy Owner Department

Education Department

Key Stakeholders		
Policy Owner:	Hariharan Devicharan	IT Manager
Reviewed by:	Margaret Haynes	Director of Schools
	Kevin Wallis	Deputy CEO
Approved by:	Dr. Shereen Gobran	Chief Executive Officer