

Data Protection Policy

Version 1.0 · Effective September 2026 · Next review September 2027

Introduction

This policy sets out the obligations of Masar University ("the University", "we", "us") regarding data protection, and the rights of learners, applicants, website visitors and other contacts ("data subjects") in respect of their personal data.

The University's online services are operated by Masar University L.L.C-FZ, Meydan Grandstand, 6th floor, Meydan Road, Nad Al Sheba, Dubai, United Arab Emirates, which is the controller of the personal data described in this policy.

The University processes personal data in accordance with the UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data, and with the EU/UK GDPR where it applies to learners located in those jurisdictions (together, "applicable data protection law").

"Personal data" means any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier, or to one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.

This policy sets out the University's obligations regarding the collection, processing, transfer, storage and disposal of personal data. It must be followed at all times by the University's employees, tutors, agents, contractors and other parties working on its behalf. The University is committed not only to the letter but also to the spirit of the law, and places high importance on the correct, lawful and fair handling of personal data, respecting the rights, privacy and trust of everyone it deals with.

Scope

This policy is published as part of the University's policies for CPD courses and professional training, and applies to personal data processed in connection with them through the website (masaruni.ae), the student information system (mysis.masaruni.ae) and the learning platform (Moodle, lms.masaruni.ae). The same principles apply to all personal data processed by the University, as described in the Privacy Policy published on masaruni.ae. Degree programmes are governed by the University's academic regulations.

Data protection principles

All personal data must be:

1. processed lawfully, fairly and in a transparent manner;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;
3. adequate, relevant and limited to what is necessary for the purposes for which it is processed;
4. accurate and, where necessary, kept up to date, with every reasonable step taken to erase or correct inaccurate data without delay;
5. kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which it is processed;
6. processed securely, with protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures.

The University is responsible for, and must be able to demonstrate, compliance with these principles.

Lawful, fair and transparent processing

The University processes personal data only where it has a lawful basis under applicable data protection law, namely where:

- the data subject has given consent to the processing for one or more specific purposes;
- the processing is necessary for the performance of a contract with the data subject, or to take steps at their request before entering into a contract;
- the processing is necessary to comply with a legal obligation of the University;
- the processing is necessary to protect the vital interests of the data subject or of another person;
- the processing is necessary for the University's legitimate interests, except where those interests are overridden by the rights and freedoms of the data subject.

Sensitive ("special category") personal data, such as information about a learner's health provided with a request for a reasonable adjustment or special consideration, is processed only where at least one of the following applies:

- the data subject has given explicit consent for one or more specified purposes;
- the processing is necessary to protect the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving consent;
- the data has clearly been made public by the data subject;
- the processing is necessary for the establishment, exercise or defence of legal claims.

Personal data we collect and why

The University collects personal data directly from data subjects and, where applicable, from third parties. It collects and processes only the data needed for the purposes of which data subjects have been informed:

- **Website visitors:** technical data such as IP address, browser and device type, and pages visited, to operate, secure and improve the website (legitimate interests).
- **People who contact us:** name, email address, telephone number and message, to answer the enquiry.
- **Applicants:** name, verified email address, telephone number, nationality, date of birth, qualifications, uploaded documents and the course or programme requested, to assess the application (steps taken at the data subject's request before a contract).
- **Enrolled learners:** the above, plus course registrations, assessment results and attendance, certificates, invoices and payments, correspondence and support tickets, to deliver courses, assess and certify learning, and collect fees (performance of the contract, and legal and accounting obligations).
- **Online payers:** transaction data such as amount, date and status. Card details are processed directly by the payment provider and are not received or stored by the University.
- **Marketing contacts:** contact details, used for marketing messages only with consent.

The University does not sell or rent personal data. It shares personal data only with service providers acting on its behalf (such as hosting, lecture streaming, payment and email providers), with competent authorities where the law requires, and with other parties where the data subject has consented.

Keeping data subjects informed

Where personal data is collected directly from data subjects, they are informed of its purpose at the time of collection, through the University's Privacy Policy and the relevant forms. Where personal data is obtained from a third party, the data subject is informed:

- when the first communication is made, if the data is used to communicate with them;
- before any transfer, if the data is to be transferred to another party; or
- in any event, as soon as reasonably possible and not more than one month after the data is obtained.

The information provided includes: the identity and contact details of the University and its Data Protection Officer; the purposes and legal basis of the processing, including any legitimate interests relied on; the categories of data concerned where it was not obtained directly; the recipients of the data; any transfers outside the United Arab Emirates and the safeguards in place; how long the data will be kept; the data subject's rights, including the

right to withdraw consent and to complain to a competent data protection authority; whether providing the data is a legal or contractual requirement and the consequences of not providing it; and any automated decision-making that will take place.

Rights of data subjects

Subject to applicable data protection law, data subjects have:

- the right to be informed;
- the right of access to their personal data and to obtain a copy of it;
- the right to rectification of inaccurate or incomplete data;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object to processing;
- rights in relation to automated decision-making and profiling;
- the right to withdraw consent at any time, where processing is based on consent, without affecting processing carried out before withdrawal.

Some records, such as academic and financial records, cannot be erased on request because the University is required to keep them.

Subject access requests

- Data subjects may make a subject access request at any time to find out what personal data the University holds about them, what it does with that data and why.
- Requests should be made in writing to the Data Protection Officer at info@masaruni.ae, preferably from the email address registered with the University. The University may ask for proof of identity before acting.
- The University responds within 30 days of receipt. Where applicable data protection law allows the period to be extended for complex or numerous requests, the data subject will be informed of the extension and the reasons within the initial 30 days.
- All subject access requests are handled by the Data Protection Officer.
- The University does not charge a fee for a normal request. It may charge a reasonable fee, where the law allows, for additional copies of information already supplied or for requests that are manifestly unfounded or excessive, particularly where they are repetitive.

Rectification, erasure, restriction and objection

Rectification

The University will rectify inaccurate or incomplete personal data, and inform the data subject, within 30 days of being told of the issue. Any third party to whom the data has been disclosed will be informed of the rectification.

Erasure

Data subjects may ask the University to erase their personal data where:

- it is no longer necessary for the purpose for which it was collected;
- they withdraw their consent and there is no other lawful basis for the processing;
- they object to the processing and there is no overriding legitimate interest to continue;
- the data has been processed unlawfully;
- erasure is needed for the University to comply with a legal obligation.

Unless the University has reasonable grounds to refuse, such as a legal duty to keep the record, requests for erasure are completed, and the data subject informed, within 30 days. Any third party to whom the data has been disclosed will be informed of the erasure, unless this is impossible or would involve disproportionate effort.

Restriction

Data subjects may ask the University to restrict the processing of their personal data. The University will then keep only the data necessary to ensure that it is not processed further, and will inform any third party to whom the data has been disclosed, unless this is impossible or would involve disproportionate effort.

Objection

Where a data subject objects to processing based on the University's legitimate interests, the University will stop that processing unless it can demonstrate compelling legitimate grounds that override the data subject's interests, rights and freedoms, or the processing is necessary for legal claims. Where a data subject objects to direct marketing, the University will stop that processing immediately.

Data retention

The University keeps personal data for no longer than is necessary for the purposes for which it was collected:

- applications that were not completed or not accepted: two years from the last update to the application;
- the academic record (courses, results and certificates): permanently, as it is the basis for issuing transcripts and verifying certificates;
- financial records: five years from the end of the financial year;
- correspondence, messages and support tickets: three years;
- website visit data: twelve months.

Records of malpractice cases are kept for at least five years, as set out in the Malpractice Policy. When a retention period ends, the data is securely deleted or anonymised.

Data security

The University protects personal data with appropriate technical and organisational measures, including:

- encrypted connections (HTTPS) for the website, the student information system and the learning platform;
- role-based access permissions, so that staff can access only the personal data they need for their duties;
- regular backups and a change log for financial and academic data;
- keeping software up to date with security updates;
- strong passwords that are never written down or shared, and locking screens when devices are left unattended;
- sharing personal data only through the University's systems and official email, never informally, and not storing it on personal devices or removable media without the approval of the Data Protection Officer;
- secure deletion of personal data that is no longer needed.

All staff, contractors and other parties working on behalf of the University who handle personal data are made aware of their responsibilities under this policy, are appropriately trained and supervised, and are bound by contract to handle personal data in accordance with it. Service providers that process personal data on the University's behalf do so under written terms that require them to protect it. The methods used to collect, hold and process personal data are regularly reviewed.

Accountability and records

The University's Data Protection Officer is responsible for overseeing the implementation of this policy and monitoring compliance with it and with applicable data protection law. The Data Protection Officer can be contacted at info@masaruni.ae.

The University keeps internal records of its processing of personal data, including: the purposes of processing; the categories of personal data and of data subjects; the service providers that process data on its behalf; any transfers of data outside the United Arab Emirates and the safeguards used; retention periods; and the security measures in place.

The Data Protection Officer oversees a data protection impact assessment before any new project or new use of personal data that is likely to present a high risk to data subjects. The assessment considers the data involved, the purposes and necessity of the processing, the risks to data subjects and to the University, and the measures proposed to address those risks.

Personal data breaches

- All personal data breaches, suspected or actual, must be reported immediately to the Data Protection Officer.
- Where a breach is likely to result in a risk to the rights and freedoms of data subjects (for example financial loss, breach of confidentiality, discrimination or reputational damage), the Data Protection Officer will ensure that the competent authority is notified without undue delay and within the timeframe required by applicable data protection law.
- Where a breach is likely to result in a high risk to data subjects, the Data Protection Officer will ensure that the affected data subjects are informed directly and without undue delay.
- Breach notifications include: the categories and approximate number of data subjects and records concerned; the contact details of the Data Protection Officer; the likely consequences of the breach; and the measures taken or proposed to address it and mitigate its effects.
- All breaches are recorded, whether or not they are notified.

Transfers of personal data outside the United Arab Emirates

The University's servers are hosted by a provider outside the United Arab Emirates, and some other service providers also process data outside the UAE. Learners also access the University's services from many countries. Personal data is transferred only in accordance with the conditions of applicable data protection law, and only to providers that are committed to protecting it appropriately, for example where:

- the destination provides an adequate level of protection for personal data;
- appropriate safeguards, such as contractual commitments, are in place;
- the data subject has given informed consent to the transfer;
- the transfer is necessary for the performance of a contract with the data subject, or for steps taken at their request before a contract;
- the transfer is necessary for legal claims, or to protect the vital interests of the data subject or another person where the data subject is unable to give consent.

Where the EU/UK GDPR applies, transfers are made only on the basis of a transfer mechanism that it recognises.

Direct marketing

Personal data is used for marketing only with the data subject's consent, which can be withdrawn at any time. The Marketing Department is responsible for ensuring that consent has been obtained and that opt-outs are respected.

Contact and complaints

Questions, requests and complaints about personal data should be sent to the Data Protection Officer:

Masar University LLC-FZ, Meydan Grandstand, 6th floor, Meydan Road, Nad Al Sheba, Dubai, United Arab Emirates

Email: info@masaruni.ae

Telephone: +966 56 546 5105

A data subject who is not satisfied with the University's response may lodge a complaint with the competent data protection authority.

Approved by: Dr. Mahmoud Elgindy

Chairman of the Board and Chief Executive Officer, Masar University

Version 1.0 · Effective September 2026 · Next review September 2027