Data Protection Policy

Personal data, privacy and your rights

Document code	MSU-POL-DPP-01	**Version**	2.0
Effective date	17 November 2026	**Next review**	17 November 2027
Document owner	Registrar's Office (Data Protection Lead)	**Approved by**	President, Madison State University
Status	Approved for use	**Applies to**	All learners, staff, agents and contractors

1. Purpose and scope

This policy explains how Madison State University ("we", "the University") protects the personal data of learners, applicants, staff, agents, contractors and other people, and the rights those people have. It applies to everyone who handles personal data for the University, in any format.

2. Legal framework and jurisdiction

Madison State University is a United States institution (Colorado) that serves learners in many countries. We apply one high standard to everyone: **UK GDPR and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025**, together with the **EU GDPR** for learners in the European Economic Area, and any other privacy law that applies where a learner lives or where we operate, including applicable US federal and state laws. Where the law of a learner's country gives stronger rights, those rights prevail. We do not claim UK or EU registration or regulatory status by following these standards.

Where the law requires us to register with a regulator, pay a fee or appoint a representative in the UK or EU, the Data Protection Lead keeps those arrangements in place and records them.

3. Roles

Role	Responsibility in this document
President	Accountable officer for this policy. Approves it, decides final-stage cases that the President was not involved in, and holds any role below that has not yet been separately assigned.
Registrar's Office	Keeps academic records, results and certificate verification data. Acts as the Data Protection Lead.
Admissions Office	First contact for enquiries and enrolment; owns marketing consent and the claims register for marketing.
Academic Quality Lead	Oversees assessment standards, internal verification, course review and learner feedback. Appointed by the President (the President acts until an appointment is made).

Data Protection Lead: the Registrar's Office, info@madisonstate.us. The Lead oversees this policy, advises on risk, keeps the records below and is the contact for individuals and regulators. All staff, agents and contractors are personally responsible for following it.

4. Principles

Personal data must be: processed lawfully, fairly and transparently; collected for specified, legitimate purposes; adequate and limited to what is necessary; accurate and kept up to date; kept no longer than necessary; and kept secure. We are responsible for showing that we comply.

5. What we hold, why and for how long

Data	Purpose	Lawful basis	Retention
Applications and identity checks	Admissions; confirm identity	Contract (taking steps at your request); legitimate interests	Unsuccessful applications: 12 months. ID images: deleted within 30 days after checking; we keep the result only

Data	Purpose	Lawful basis	Retention
Academic records, results and certificates	Run programmes; issue and verify certificates for life	Contract; legitimate interests; legal obligation	Permanent (needed to verify certificates)
Payments and invoices	Take and record payment; refunds	Contract; legal obligation	7 years. We do not store full card numbers
Learning platform data	Deliver learning; support; improve courses	Contract; legitimate interests	2 years after last activity
Recordings of live, oral or proctored assessments	Assessment integrity; appeals evidence	Legitimate interests (with notice); consent where required	12 months after the decision, longer while a case is open
Complaints and appeals	Investigate and improve	Legitimate interests; legal obligation	6 years after closure
Safeguarding records	Protect people at risk	Legal obligation; vital interests; public interest	7 years after the last action, or as the law requires
Marketing contacts	Send news and offers	Consent	Until consent is withdrawn, or 24 months without engagement
Staff, agent and contractor data	Manage the relationship	Contract; legal obligation	Duration of the relationship plus 6 years

This retention schedule is reviewed each year. Special category data (for example health information in an adjustment request) is processed only where the law allows, with extra safeguards, and shared only with people who need it.

6. Your rights

You have the right to be informed; to access your data; to have inaccurate data corrected; to have data erased; to restrict or object to processing; to data portability; to withdraw consent at any time; and not to be subject to a decision based solely on automated processing that has a legal or similarly significant effect. We make no such solely automated decisions: if a tool flags something, such as a possible integrity concern, a trained person reviews it and decides.

- **Requests** go to the Data Protection Lead. We acknowledge them within **7 days** and respond within **one month**. We may extend by up to two further months for complex requests, and tell you why. We may ask you to clarify the request or confirm your identity, and we carry out reasonable and proportionate searches.
- There is no charge unless a request is manifestly unfounded or excessive.
- You may opt out of marketing at any time using the link in a message or by emailing the Admissions Office.

7. Data protection complaints

If you are unhappy with how we handle your data, tell the Data Protection Lead at info@madisonstate.us. We acknowledge your complaint within 7 days, investigate without undue delay, tell you the outcome, and explain the next step. If you are still unhappy, you may complain to the regulator for your country, for example the UK Information Commissioner’s Office, your national data protection authority in the EEA, or the competent authority where you live.

8. Online learning, recordings and artificial intelligence

- We tell learners before a session is recorded and why, and who may view it.
- Before we introduce proctoring, remote identity verification or any similar tool, we carry out a data protection impact assessment. We use the least intrusive method that meets the purpose, and offer an alternative to learners who cannot or do not wish to use it, where that is possible.
- We do not use facial recognition to identify learners unless the learner gives explicit consent and an alternative is available.
- Staff must not enter personal data into public AI tools. Only tools approved by the Data Protection Lead, with suitable data processing terms, may be used with personal data, and learners are told when such a tool is used on their work.

9. Third parties and international transfers

- Every supplier that handles personal data for us (for example learning platform, email, payment, cloud hosting and communications providers) is checked before use and bound by a written contract with data protection terms. The Registrar’s Office keeps a list.
- Authorised agents who receive learner data must follow this policy under their written agreement and may use the data only for the agreed purpose.
- We transfer personal data outside the UK or EEA only where an adequacy decision, standard contractual clauses or another approved safeguard applies, and where the risks have been assessed.

10. Security

- Access is limited to those who need it, with multi-factor authentication for administrator accounts.
- Data is encrypted in transit and at rest, and backed up.
- Work devices are managed. Personal devices are used only where approved and secured. Personal data is not stored on unmanaged devices or in unapproved services.
- Paper records are avoided; where used they are locked away and posted only by tracked methods.
- Data is deleted or destroyed securely at the end of its retention period.

11. Personal data breaches

Anyone who discovers or suspects a breach reports it to the Data Protection Lead immediately and within 24 hours at the latest. The Lead assesses the risk, contains the breach, and records it in the breach log. If the breach is likely to result in a risk to individuals, we notify the relevant regulator within **72 hours** of becoming aware, where the law requires it. If the risk is high, we tell the affected people without undue delay. We review every breach for lessons.

12. Records, impact assessments and design

The Registrar’s Office keeps a record of processing activities, a privacy notice, a data sharing log and the breach log. A data protection impact assessment is carried out before any new high-risk processing. New systems are designed to protect privacy by default.

13. Children and vulnerable people

Our programmes are designed for adult learners. We do not knowingly collect data from children under 13. Where a learner is under 18, we apply extra safeguards and follow the Safeguarding Learner Policy.

14. Marketing and electronic communications

The Admissions Office is responsible for obtaining and recording consent for marketing, and for honouring opt-outs promptly. We comply with the electronic marketing and anti-spam laws that apply to each recipient.

15. Certificate verification

Our public verification service shows only the minimum information needed to confirm a certificate (for example name, programme, graduation date and status), and only to a person who has the certificate number and verification code. It never shows date of birth, contact details or marks.

16. Training, monitoring and consequences

All staff, agents and contractors who handle personal data complete data protection training when they start and every year. The Data Protection Lead audits compliance at least yearly and reports to the President. A breach of this policy may lead to disciplinary action or termination of an agreement.

17. Contact

Data Protection Lead (Registrar’s Office), Madison State University, 282 Ptarmigan St, Golden, CO 80403, USA. Email info@madisonstate.us. Telephone +1 (608) 572-7547.

18. Related documents

Complaints Policy · Safeguarding Learner Policy · Malpractice Policy · Responsible Marketing Procedure · Reasonable Adjustments Policy.

19. Approval and review

This document was approved by the President of Madison State University. It is reviewed at least once a year, and sooner if the law, our accreditation context or a serious incident requires it. The Academic Quality Lead keeps the change log.

Name	Mohammed Khalaf
Position	President, Madison State University
Date	17 November 2026
Signature	
Next review date	17 November 2027

Change log: Version 2.0, 17 November 2026. Full revision following an external governance review (jurisdiction statement, unified roles, fair timelines, online-learning provisions, document control).