



Institute for  
Advanced Learning  
& Metacognition

**INSTITUTE FOR ADVANCED LEARNING AND METACOGNITION**

*Advancing the Science of Learning*

# GDPR and Data Protection Policy

---

Policy and Procedures

**Version 1.0** • Status: Adopted

Date: 24<sup>th</sup> June 2026

Registered charity number: 1189445

*Approved by the Board of Trustees on 16<sup>th</sup> June 2026*

## Document Control

Version	Date	Author	Description	Review date
0.1	15/06/26		Initial draft for review by the Trustees	—
1.0	16/06/26	Board of Trustees	Adopted by the Board of Trustees	16/06/26

## Approval and Review

Approved by	Role	Date	Signature
Fabian Lord	Chair of the Board of Trustees	24 <sup>th</sup> June 2026	

## Contents

1. Purpose.....	3
2. Scope .....	3
3. Data protection principles .....	3
4. Lawful bases for processing .....	3
4.1 Special category data .....	4
5. Individual rights .....	4
6. Data security and breach management .....	4
6.1 Reporting a data breach .....	4
7. Data retention .....	5
8. Roles and responsibilities .....	5
9. Related policies and legislation .....	5
10. Monitoring and review.....	6

## 1. Purpose

The Institute for Advanced Learning and Metacognition (IALM) is committed to protecting the privacy and security of personal data. As a professional research and educational body, we process personal data relating to our members, learners, staff, volunteers and partners.

The purpose of this Data Protection (GDPR) Policy (the “Policy”) is to:

- ensure IALM complies with the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR);
- protect the rights and freedoms of the individuals whose data we process;
- provide a clear framework for the lawful, fair and transparent handling of personal data; and
- establish accountability and security measures to prevent and manage data breaches.

## 2. Scope

This Policy applies to all personal data processed by IALM, regardless of format or storage method. It applies to all trustees, employees, volunteers, consultants and partners who process personal data on behalf of the Institute.

## 3. Data protection principles

IALM adheres to the seven principles of data protection set out in the UK GDPR:

1. Lawfulness, fairness and transparency — data is processed lawfully, fairly and transparently.
2. Purpose limitation — data is collected for specified, explicit and legitimate purposes.
3. Data minimisation — we collect only data that is adequate, relevant and necessary.
4. Accuracy — we take reasonable steps to keep data accurate and up to date.
5. Storage limitation — data is kept only for as long as necessary.
6. Integrity and confidentiality — data is processed securely against unauthorised access, loss or damage.
7. Accountability — IALM is responsible for, and must be able to demonstrate, compliance with these principles.

## 4. Lawful bases for processing

IALM will only process personal data where at least one of the following lawful bases applies:

- **Contractual necessity** — to perform a contract with an individual (for example, administering membership or delivering a course);
- **Legal obligation** — to comply with a legal requirement (for example, tax reporting or safeguarding duties);
- **Legitimate interests** — for the Institute’s legitimate activities, provided these do not override the individual’s rights (for example, sending professional updates to members);
- **Consent** — where an individual has given clear, affirmative consent for a specific purpose (for example, marketing or case studies);
- **Vital interests** — to protect someone’s life in an emergency; and
- **Public task** — for tasks carried out in the public interest (for example, certain research activities).

#### 4.1 Special category data

Processing of special category (sensitive) data — such as data concerning health, ethnicity or religious belief — requires additional protection, and will only be carried out where a specific condition applies, such as explicit consent or substantial public interest (for example, monitoring equality and diversity).

## 5. Individual rights

Under the UK GDPR, individuals have the following rights:

- **the right to be informed** about how their data is used (through our privacy notices);
- **the right of access** to a copy of their personal data (a Subject Access Request);
- **the right to rectification** of inaccurate data;
- **the right to erasure** in certain circumstances (the “right to be forgotten”);
- **the right to restrict processing** of their data;
- **the right to data portability** in a structured, machine-readable format; and
- **the right to object** to their data being used for certain purposes (for example, direct marketing).

IALM will respond to all rights requests within the statutory timeframe (usually one month).

## 6. Data security and breach management

IALM implements appropriate technical and organisational measures to keep personal data secure, including access controls, secure storage, and training for those who handle data.

### 6.1 Reporting a data breach

A personal data breach is any security incident leading to the accidental or unlawful loss, alteration, or unauthorised disclosure of personal data.

- All suspected breaches must be reported to the Institute's Data Protection Lead immediately.
- If a breach is likely to result in a risk to individuals, IALM will notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of it.
- Where the risk to individuals is high, affected individuals will also be informed without undue delay.

## 7. Data retention

IALM will not keep personal data for longer than is necessary. Our typical retention periods include:

- **Membership records:** retained for the duration of membership plus six years, for financial and audit purposes;
- **Learning and qualification records:** retained for as long as necessary to verify professional status or membership history, or to provide replacement records;
- **Recruitment data:** retained for six months for unsuccessful candidates.

Full details are set out in the Institute's Records Retention Schedule.

## 8. Roles and responsibilities

- **The Board of Trustees** holds ultimate responsibility for data protection compliance.
- **The Data Protection Lead** (or Data Protection Officer, where the Institute is required to appoint one) monitors compliance, provides advice, and acts as the point of contact for data protection matters and for the ICO.
- **All staff and volunteers** are responsible for following this Policy and reporting any security concerns.

IALM is registered with the Information Commissioner's Office (ICO) as a data controller (registration number: ZC173366).

## 9. Related policies and legislation

- Data Protection Act 2018 and the UK GDPR;
- the Privacy and Electronic Communications Regulations (PECR);
- IALM Privacy Policy (the Institute's public-facing privacy notice);
- IALM Records Retention Schedule; and
- IALM information security arrangements.

## 10. Monitoring and review

This Policy will be reviewed by the Board of Trustees at least annually, or sooner if required by changes in data protection law, to ensure it remains effective and compliant.