MIAG

DATA PROTECTION & GDPR POLICY

MIAG ORGANISATIONAL POLICY

Organisation-wide

Supporting consistent, effective practice across the MIAG organisation.

SUPPORTING INDIVIDUALS | CREATING OPPORTUNITIES | ENRICHING COMMUNITIES

Policy Statement:

MIAG (Meeting Individual Aspirations & Goals) is committed to protecting the personal information entrusted to us by learners, parents/carers, staff, governors, commissioners, professionals, applicants and other stakeholders. Personal data must be processed lawfully, fairly, transparently and securely, with particular care where information relates to children, safeguarding, health, SEND or other special category data.

This policy sets out the organisational expectations for the collection, use, sharing, storage, retention and disposal of personal data. It applies alongside MIAG safeguarding arrangements and is intended to support a culture in which data protection is part of everyday professional practice rather than a separate administrative task.

Purpose and Scope:

The purpose of this policy is to ensure that MIAG:

- has clear accountability for the information it processes;
- processes personal data only for lawful, specified and legitimate purposes;
- uses the minimum information necessary and keeps it accurate and up to date;
- protects confidentiality, integrity and availability through appropriate technical and organisational measures;
- understands and responds appropriately to data protection rights, incidents and complaints; and
- can demonstrate compliance through normal business records, monitoring, review and organisational learning.

This policy applies to all MIAG employees, governors, volunteers, agency workers, contractors and other individuals who process personal data on behalf of MIAG, and to all personal data processed by MIAG in any format.

Key Principles:

- Lawfulness, fairness and transparency – individuals should understand how and why their information is used
- Purpose limitation – information is collected for specified, explicit and legitimate purposes and is not used incompatibly with those purposes
- Data minimisation – only information that is adequate, relevant and necessary is collected and used
- Accuracy – reasonable steps are taken to keep personal information accurate and current
- Storage limitation – information is retained only for as long as necessary, in line with MIAG retention arrangements and legal requirements
- Integrity and confidentiality – information is protected against unauthorised or unlawful processing, loss, destruction or damage
- Accountability – MIAG must be able to demonstrate that these principles are applied in practice

Lawful Processing:

Before collecting, using or sharing personal data, staff must understand the purpose and identify the appropriate lawful basis. Depending on the circumstances, this may include consent, contractual necessity, legal obligation, public task, vital interests, legitimate interests or another lawful basis available under current data protection legislation.

Consent must not be treated as the default where another lawful basis is more appropriate. Where consent is relied upon, it must be freely given, specific, informed and capable of being withdrawn.

Special category data, including health, racial or ethnic origin and other protected categories, requires both a lawful basis under Article 6 and an applicable condition under Article 9 of the UK GDPR. Safeguarding and health information must be handled on a strict need-to-know basis.

Children, Safeguarding and Information Sharing:

MIAG recognises that data protection legislation is not a barrier to safeguarding. Where information needs to be shared to protect a child or promote their welfare, staff should act promptly, use professional judgement and follow MIAG safeguarding and information-sharing procedures. KCSIE 2026 reinforces that data protection should not prevent necessary safeguarding information sharing and expects safeguarding records to capture actions, decisions, rationale and outcomes.

When sharing information, staff should consider what is necessary, proportionate and relevant, who needs to receive it, how it will be shared securely, and what record of the decision is required. Where there is uncertainty, staff should seek advice from the DSL/DDSL and/or the DPO as appropriate.

Data Collection, Privacy and Transparency:

- MIAG will provide appropriate privacy information explaining what personal data is collected, why it is used, the relevant lawful basis, who it may be shared with, retention and individual rights
- Personal data must not be collected simply because it may be useful in the future
- Staff must use approved MIAG systems and communication methods when processing personal data and must take particular care when sending information by email or messaging platforms
- Photographs, videos, CCTV and other recordings involving identifiable individuals must be processed in accordance with the relevant MIAG arrangements and permissions/lawful bases
- Where MIAG introduces new technology, systems or processing that may present a high risk to individuals, privacy and data protection must be considered at the design stage and a Data Protection Impact Assessment (DPIA) completed where required

Security and Access:

Access to personal data is restricted according to role and legitimate need. Staff are responsible for protecting information in their care, including passwords, devices, paper records and digital files.

- Do not share passwords or leave systems open and unattended
- Use locked storage for paper records containing personal data
- Use approved, secure systems for electronic records and communication
- Check recipients and attachments carefully before sending emails or documents
- Avoid discussing confidential information where it can be overheard
- Report lost devices, misdirected information, unauthorised access or other suspected incidents immediately

Data Breaches and Information Security Incidents:

A suspected or actual personal data breach must be reported immediately to the DPO/Data Protection Lead. This includes information sent to the wrong person, accidental disclosure, loss or theft of equipment or records, unauthorised access, or insecure disposal.

The DPO will assess and document the incident, including the nature of the breach, affected data and individuals, likely consequences, actions taken and whether notification is required. Where a breach is likely to result in a risk to individuals' rights and freedoms, the ICO must normally be notified without undue delay and, where feasible, within 72 hours of becoming aware of the breach.

MIAG will maintain a Data Protection Incident/Breach Register and retain appropriate evidence of decisions and actions. Where a breach indicates a weakness in practice, the response will include learning and improvement actions rather than treating the incident as an isolated event.

Data Breaches will be reported to the relevant Governing Body/Management Board by the Head Teacher/Provision Lead.

Data Protection Complaints:

From 19 June 2026, organisations have a statutory duty to provide a clear means for individuals to complain about the handling of their personal data. MIAG will provide an accessible route for data protection complaints, acknowledge complaints within 30 days, investigate appropriately and communicate the outcome without undue delay.

Complaints will be recorded and reviewed by the DPO/Data Protection Lead, with escalation to the appropriate senior leader and/or the ICO where appropriate.

Individual Rights:

MIAG will respect the rights provided by data protection law. Depending on the circumstances, individuals may have rights including:

- the right to be informed about processing;
- the right of access to personal data;
- the right to rectification;
- the right to erasure, where applicable;
- the right to restrict processing;
- the right to object to certain processing;
- rights relating to data portability, where applicable; and
- rights relating to automated decision-making and profiling, where applicable.

Requests will be handled in accordance with current ICO guidance and the circumstances of the request. Subject Access Requests (SAR) should be directed to the COO/DPO/Data Protection Lead in accordance with MIAG's operational procedure. Staff must not disclose information directly in response to a formal rights request unless authorised to do so.

Records, Retention and Disposal:

MIAG will retain personal data only for as long as there is a legitimate and documented reason to do so. Retention periods will reflect statutory requirements, regulatory expectations, contractual requirements and the operational needs of MIAG.

Safeguarding and child protection records require particular care and must be retained and transferred in accordance with current KCSIE requirements and MIAG safeguarding procedures. Records must be securely deleted, destroyed or otherwise disposed of when the retention period ends.

MIAG will maintain appropriate records of processing, policies, procedures, incidents, complaints, rights requests, DPIAs and other evidence needed to demonstrate accountability.

Data Sharing and Third Parties:

MIAG may share personal data with Local Authorities, commissioners, schools and colleges, social care, health professionals, safeguarding partners, examination bodies, regulators and other organisations where there is a lawful and appropriate reason to do so.

Before sharing, staff must consider the lawful basis, necessity, proportionality, recipient, security and any additional safeguards required. Information about children requires particular care and the best interests of the child should be a primary consideration.

Where a third party processes personal data on MIAG's behalf, appropriate contractual and data protection arrangements must be in place. Staff must not introduce new systems, apps or platforms that process MIAG personal data without appropriate authorisation and data protection consideration.

Staff Responsibilities and Training:

All staff are responsible for following this policy and completing required data protection training. Staff must understand that accidental disclosure is still a data protection incident and should be reported immediately rather than attempting to resolve or conceal it themselves.

Head Teachers/Provision Leads are responsible for reinforcing good practice, responding to concerns and ensuring that staff understand local arrangements. The DPO/Data Protection Lead provides advice, oversight and escalation in relation to data protection matters and maintains appropriate independence from operational decisions where required by law.

Governance, Monitoring and Assurance:

The COO/DPO will oversee organisational data protection compliance and report significant issues, trends, breaches, complaints and improvement actions through the MIAG governance and assurance arrangements.

The MIAG Framework for Excellence and associated Dashboard will provide the organisational assurance mechanism, linking policy, practice, recording, review, learning and improvement. Monitoring will consider whether arrangements are implemented consistently and whether actions arising from incidents or reviews have been completed and embedded.

Relevant evidence should be available through normal MIAG business processes. This is consistent with the September 2026 Ofsted approach for non-association independent schools, which states that inspectors will consider how systems and processes operate in practice and should not expect schools to create inspection-specific paperwork.

Document Control Detail

Document	Data Protection & GDPR Policy
Policy Type	MIAG Organisational Policy
Policy Owner	Lisa Savage, COO
Approved By	Guy Hopson
Approval Date	8th September 2026
Effective From	1 September 2026
Review Date	August 2027

Version History

Version	Date	Summary of Change
2.0	September 2026	Updated as a MIAG Organisational Policy to reflect current UK data protection requirements, the Data (Use and Access) Act 2025, KCSIE 2026, revised ISS guidance and the Ofsted inspection framework for non-association independent schools from September 2026.

MIAG ~ Meeting Individual Aspirations & Goals