

MIAG



ONLINE SAFETY & INTERNET POLICY

MIAG ORGANISATIONAL POLICY

Organisation-wide policy

This policy applies across MIAG and forms part of the MIAG Organisational Policy Framework.

Policy Statement:

MIAG (Meeting Individual Aspirations & Goals) is committed to providing a safe, secure and well-managed digital environment that safeguards and promotes the welfare of children and young people, while enabling technology to support learning, communication and organisational effectiveness.

Online safety is a safeguarding responsibility. MIAG recognises that online risks change rapidly and that effective safeguarding requires a combination of education, professional supervision, appropriate technology, clear expectations, effective filtering and monitoring, and prompt action when concerns arise.

Purpose and Aims:

- ❖ Protect children and young people, staff and other users from online harm, abuse, exploitation and inappropriate content
- ❖ Support learners to develop the knowledge, skills, confidence and resilience to use technology safely and responsibly
- ❖ Ensure digital systems, devices, platforms and online communication are used appropriately and securely
- ❖ Maintain effective filtering and monitoring arrangements that reflect MIAG's risk profile and safeguarding responsibilities
- ❖ Ensure online safeguarding concerns are identified, reported, recorded and responded to appropriately
- ❖ Provide a clear organisational framework which can be supported by provision-specific arrangements where local practice or risk requires additional detail

Scope:

This policy applies across MIAG to all employees, Directors/Governors, volunteers, agency and supply staff, contractors, learners and visitors, as appropriate to their role.

It applies to MIAG-owned or managed devices, networks, systems, accounts and platforms and to online activity undertaken through MIAG systems or in connection with MIAG provision, including remote learning and off-site activity where relevant.

Provision-specific procedures may set out local arrangements, including device use, acceptable use, filtering and monitoring contacts, reporting routes and responses to particular risks.

Legislative and Regulatory Framework

This policy is read alongside the legislation and statutory guidance applicable to MIAG and its provisions. The key framework includes:

- ❖ Keeping Children Safe in Education 2026 (KCSIE), effective from 1 September 2026

- ❖ Education (Independent School Standards) Regulations 2014 and current DfE Independent School Standards guidance
- ❖ Data Protection Act 2018 and UK GDPR, including changes arising from the Data (Use and Access) Act 2025
- ❖ Counter-Terrorism and Security Act 2015 and the Prevent duty guidance for England and Wales
- ❖ Equality Act 2010
- ❖ Online Safety Act 2023, where relevant to the online services and platforms used by or accessed by learners
- ❖ Current Department for Education filtering and monitoring, cyber security and digital technology standards and associated guidance

Roles and Responsibilities:

Role	Key responsibility
Proprietor / COO/Directors / Governors	Provide strategic oversight and assurance that appropriate online safeguarding, filtering and monitoring arrangements are in place and effective
Headteacher / Senior Leader	Ensure the policy is implemented, that appropriate resources and arrangements are in place, and that identified actions are followed through
Designated Safeguarding Lead (DSL)	Lead on safeguarding matters arising from online activity and filtering/monitoring alerts; ensure concerns are assessed, recorded and responded to through safeguarding procedures
IT / Technical Support	Maintain technical systems, filtering and monitoring, provide appropriate reports, support reviews and act on technical issues and agreed actions
All Staff	Model safe and professional technology use, supervise learners appropriately, understand reporting arrangements and report safeguarding concerns promptly
Learners	Use technology safely, respectfully and in accordance with MIAG expectations, and report concerns or harmful content
Parents / Carers	Support safe and responsible use of technology and engage with MIAG where online safety concerns affect a learner

Acceptable and Professional Use:

MIAG expects technology to be used in a way that supports learning, professional practice, safeguarding and respectful communication.

- ❖ Users must access only systems, platforms and content that are authorised and appropriate for their role
- ❖ Passwords, authentication information and personal data must be kept secure and must not be shared inappropriately
- ❖ Users must not deliberately bypass or disable filtering, monitoring, security controls or other technical safeguards
- ❖ Learners must report harmful, inappropriate or concerning online content or contact to a trusted adult
- ❖ Staff must maintain professional boundaries and must use approved MIAG systems and accounts when communicating with learners
- ❖ Staff must not use personal social-media accounts or personal messaging services to communicate with learners
- ❖ Personal devices must only be used in accordance with MIAG policy and provision-specific arrangements

Online Safety Risks:

MIAG recognises that online safeguarding risks may include, but are not limited to:

- ❖ Cyberbullying, online abuse and harmful communications
- ❖ Grooming, exploitation, sexual abuse, sexual harassment and inappropriate contact
- ❖ Exposure to pornography, violence, extremist or terrorist material and other harmful content
- ❖ Self-harm, suicide-related content and content that encourages harmful behaviours
- ❖ Radicalisation, extremism and harmful ideological influence
- ❖ Misinformation, disinformation and harmful online influence
- ❖ Online fraud, identity theft, phishing, malware and other cyber threats
- ❖ Excessive or unsafe online behaviour, gaming, social-media use or other digital activity
- ❖ Risks associated with generative artificial intelligence, including inappropriate content, misinformation, privacy risks, manipulation and misuse of personal data

Filtering and Monitoring:

MIAG will maintain filtering and monitoring arrangements that are appropriate to the age, needs and risk profile of learners and the way technology is used within each provision.

- ❖ Filtering is preventative and should block illegal, inappropriate and potentially harmful content while avoiding unreasonable restriction of teaching and learning
- ❖ Monitoring is reactive and should identify activity or behaviour that may indicate safeguarding, inappropriate-use or technical concerns
- ❖ Filtering and monitoring responsibilities will be clearly allocated between senior leadership, safeguarding and technical support
- ❖ The DSL and relevant technical staff will work together to review alerts and respond to safeguarding concerns
- ❖ Filtering and monitoring provision will be reviewed at least annually and sooner where there is a significant safeguarding incident, material change in technology or working practice, or a change in learner risk
- ❖ Checks of filtering arrangements will be recorded, including the date, person undertaking the check, what was tested and any actions identified
- ❖ Where technical monitoring is used, MIAG will maintain an incident-response process, including regular review of monitoring reports and immediate escalation of high-risk safeguarding concerns
- ❖ All users will be informed that filtering and monitoring are in operation, in a manner appropriate to their age and role

Technical Safeguards and Cyber Security:

- ❖ Secure firewalls and appropriate network protection
- ❖ Secure authentication, password and access-control arrangements
- ❖ Appropriate anti-malware and endpoint protection
- ❖ Regular security updates and vulnerability management
- ❖ Restricted administrative access
- ❖ Appropriate audit logs and usage records
- ❖ Network and device arrangements that support appropriate separation of user groups and protection of learner and organisational data
- ❖ Risk assessment and assurance before introducing new technologies, platforms or significant technical changes

MIAG will work towards and maintain the Department for Education's applicable digital and technology standards, including filtering and monitoring and cyber security standards, proportionately to the needs and circumstances of each provision.

Personal Devices, BYOD and Mobile Technology:

The use of personal devices or bring-your-own-device (BYOD) arrangements will only be permitted where authorised and where appropriate safeguards are in place. Learner and staff personal devices

must not be used in ways that undermine filtering, monitoring, professional boundaries, confidentiality or safeguarding.

Staff **must not** use personal devices to communicate privately with learners or to capture or store learner images or information unless an explicitly authorised MIAG process permits this and the relevant data protection and safeguarding requirements are met.

This policy should be read alongside the MIAG Mobile Phone & Smart Technology Policy and any provision-specific arrangements.

Social Media and Online Communication:

- ❖ Staff must maintain appropriate professional boundaries online and must not engage with learners through personal social-media accounts
- ❖ MIAG communication with learners and families should use approved organisational systems and channels
- ❖ Staff must consider whether their online behaviour could reasonably undermine professional trust, safeguarding or confidence in their role
- ❖ Learners will be supported to understand privacy, digital footprints, respectful communication, consent and the potential consequences of sharing content

Remote Learning and Online Platforms:

- ❖ Online platforms used for learning or communication must be approved and appropriately risk-assessed
- ❖ Where one-to-one online interaction is necessary, it must be planned, authorised, professionally conducted and appropriately visible or auditable
- ❖ Staff must maintain professional standards equivalent to those expected in face-to-face practice
- ❖ Appropriate supervision, access controls and safeguarding arrangements must be applied
- ❖ Any recording of online sessions must have a clear purpose, lawful basis, appropriate notice and secure storage arrangements

Online Safety Education and Support

Online safety education forms part of MIAG's wider safeguarding and personal development work. It will be age-, ability- and developmentally appropriate and will take account of the needs of learners with SEND and other vulnerabilities.

- ❖ Learners will be taught how to recognise and manage online risks and how to seek help
- ❖ Staff will receive appropriate safeguarding and online safety training and updates
- ❖ Parents and carers will be provided with information and support to help them understand and manage online risks

- ❖ Targeted support will be provided where a learner's vulnerability, circumstances or online behaviour indicates an increased level of risk

Generative AI and Emerging Technology:

MIAG recognises that generative AI and other emerging technologies can provide educational and organisational opportunities but may also create safeguarding, privacy, accuracy, bias, copyright, security and wellbeing risks.

- ❖ New AI-enabled tools must be appropriately risk-assessed before use with or for learners
- ❖ Personal or sensitive information must not be entered into AI tools unless the use has been approved and is lawful, necessary and appropriately protected
- ❖ Staff and learners must be supported to understand the limitations of AI-generated content, including misinformation and fabricated information
- ❖ MIAG will consider the Department for Education's product safety standards and current digital and technology guidance when introducing or reviewing AI tools

Data Protection and Privacy:

Online safety arrangements must operate consistently with data protection law. MIAG will process monitoring, filtering, safeguarding and user information lawfully, fairly and proportionately.

- ❖ Access to monitoring information will be restricted to authorised staff
- ❖ Monitoring data will be retained only for as long as necessary and in accordance with MIAG retention arrangements
- ❖ A Data Protection Impact Assessment (DPIA) will be completed before introducing a new filtering or monitoring system or making significant changes where required
- ❖ Privacy information will explain what is monitored, why it is monitored, who may access alerts or reports and how long relevant information is retained
- ❖ Third-party providers will be appropriately assessed and their data protection arrangements reviewed

Reporting and Responding to Concerns:

Any online safety or safeguarding concern must be reported promptly through MIAG's safeguarding arrangements. This includes concerns arising from filtering or monitoring alerts, staff observation, learner disclosure, parent/carers information or other intelligence.

- ❖ Concerns will be recorded appropriately and passed to the DSL or nominated safeguarding lead
- ❖ The DSL will determine the appropriate safeguarding response and referral route
- ❖ Technical incidents will be escalated to IT support where appropriate
- ❖ External agencies will be involved where required by the circumstances or statutory duties

- ❖ Serious incidents and emerging themes will be reviewed to identify learning, preventative action and any required changes to practice or technical controls

Breaches of Policy:

Misuse of technology may result in proportionate action under MIAG's behaviour, safeguarding, disciplinary or other relevant procedures. The response will reflect the nature, seriousness and impact of the incident.

- ❖ Learner misuse may result in education, restricted access, behaviour consequences and/or safeguarding intervention
- ❖ Staff misuse may result in management or disciplinary action and, where appropriate, referral to external agencies or professional bodies
- ❖ Serious incidents may require immediate safeguarding, data protection or cyber-security action

Monitoring, Assurance and Review:

The effectiveness of this policy will be reviewed through a combination of filtering and monitoring assurance, safeguarding records, incident trends, staff and learner feedback, technical reviews and relevant governance oversight.

- ❖ Filtering and monitoring arrangements will be reviewed at least annually
- ❖ The policy will be reviewed annually or sooner where legislation, statutory guidance, technology or MIAG practice changes
- ❖ Directors/Governors will receive appropriate assurance on filtering and monitoring effectiveness, significant incidents, emerging risks and agreed actions
- ❖ Provision-specific arrangements will be reviewed alongside local safeguarding and technology arrangements

Document Control:

Document Control	Details
Policy	Online Safety & Internet Policy
Policy Type	MIAG Organisational Policy
Policy Owner	Lisa Savage, COO
Approved By	Guy Hopson
Approval Date	27/08/26
Effective From	1 September 2026
Review Date	August 2027
Version	1.0
Applies To	MIAG organisation-wide

Version	Date	Summary of Change
1.0	26/08/26	Updated and reformatted to reflect current legislation, KCSIE 2026, DfE filtering and monitoring standards, current data protection requirements and MIAG organisational arrangements.

MIAG – Meeting Individual Aspirations & Goals