Aspire
FOUNDATION

Information Governance, Data Protection and Security Policy

Approved January 2026
Review December 2026

1. Purpose

To ensure all Aspire Foundation information (about children, families, staff, volunteers, partners, and operations) is handled lawfully, ethically, securely, and effectively.

This policy defines how information is created, classified, stored, accessed, shared, transmitted, retained, and disposed of, safeguarding confidentiality, integrity, and availability (CIA).

2. Scope

Applies to:

- People: all staff, volunteers, trustees, contractors, and third parties with access to Aspire Foundation information.
- Information types: paper records, electronic files, emails, photos, audio/video, online platforms, phone calls, and spoken information.
- Locations: offices, partner sites, remote/home working, mobile devices, cloud services.

3. Legal & Regulatory Framework (UK)

Aspire Foundation complies with:

- UK General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 2018)
- Privacy and Electronic Communications Regulations (PECR)
- Data (Use and Access) Act 2025 (DUAA) - including changes on recognised legitimate interests, automated decision-making safeguards, “reasonable and proportionate” subject access requests (SAR) search standards, and cookie/consent flexibilities (as applicable)
- Computer Misuse Act 1990, Freedom of Information Act 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998, Copyright, Designs and Patents Act 1988, Telecommunications (Lawful Business Practice) Regulations 2000, Civil Contingencies Act 2004

Email security must follow UK best practice (TLS, DMARC/DKIM/SPF, MTA-STS, inbound DMARC enforcement). Encryption is an appropriate technical measure under UK GDPR Article 32 and must be used wherever proportionate to risk.

4. GDPR Principles (Information Governance & Data Protection)

- Lawfulness, Fairness & Transparency
- Purpose Limitation
- Data Minimisation
- Accuracy
- Storage Limitation
- Integrity & Confidentiality (security by design and default)

- Accountability—evidence compliance via records, Data Protection Impact Assessments (DPIAs), retention schedules, training logs

5. Roles & Responsibilities

- Board/Trustees/SMT: Oversight, resourcing, risk management, approval, and monitoring.
- Data Protection Officer (DPO) – GCC Schools Data Protection Office (schoolsdpo@gloucestershire.gov.uk): Advice, audits, DPIAs, SARs, breaches, Information Commissioner's Office (ICO) liaison.
- Managers: Implement controls; ensure team compliance and training.
- All staff/volunteers: Follow policy/procedures, protect information, report incidents immediately.
- Third parties/processors: Comply via contracts/DPAs with UK GDPR/DPA/PECR and our requirements.

6. Definitions

- Personal data: Information identifying a living person.
- Special category data: Sensitive data (e.g., health, ethnicity, religion, biometric) with extra protections.
- Processing: Any operation on data (collection, storage, sharing, erasure, etc.).
- Controller/Processor/Data Subject/Consent: As defined under UK GDPR.
- Recognised Legitimate Interests (DUAA): Statutory lawful basis for defined activities (e.g., security, fraud prevention, certain charitable direct marketing) where conditions are met.

7. Legal Bases for Processing

- Legal obligation (e.g., safeguarding, health & safety, statutory returns)
- Contractual necessity (e.g., employment, childcare agreements)
- Public task (where applicable)
- Consent (specific, informed, withdrawable)
- Recognised Legitimate Interests (DUAA) for defined activities (e.g., network/security operations and certain charity direct marketing under soft opt-in)
- For special category data, an additional condition (e.g., explicit consent, vital interests, statutory obligations) must be met.

8. Children's Data: Specific Considerations

- Children under 18 have the same UK GDPR rights; competence may allow them to exercise rights themselves.
- Parental/guardian consent is obtained where required.
- Provide age-appropriate privacy notices.
- Consider the child's best interests in all processing decisions.

9. What Data We Collect and Why

Category	Examples	Purpose / Use
Child's names, date of birth, home address, next of kin details	Admission records	Care planning, emergency contact, attendance etc.
Health information (allergies, medical conditions)	Health forms, information from parents/carers	Safety, health and wellbeing needs.
Photographs / videos	For displays, portfolios, newsletters, website (if consented)	Monitoring progress, celebrating achievements, promoting the centre.
Attendance, developmental assessments etc.	Observation records, learning journals	Supporting learning and development, statutory requirements.
Staff data	Employment contract, payroll, qualifications	Employment, legal compliance, performance management.
Parent/carer contact data	Phone, email, address	Communication, invoices etc.

10. Information Classification

- Public: May be openly shared (e.g., marketing).
- Internal: For Aspire staff/volunteers (e.g., memos, rotas).
- Confidential: Sensitive/personal (e.g., safeguarding reports, children's records, HR). Confidential must always be stored/transmitted securely.

11. Security Controls (CIA)

11.1 Physical & Paper

- Store confidential files in locked cabinets or restricted areas; never leave unattended.
- Supervise visitors; control building access; lock offices and cabinets.
- Use secure disposal (shredding, certified destruction).

11.2 Electronic

- Role-based access control (RBAC) and least privilege.
- Password protection and multi-factor authentication (MFA) for remote access and privileged accounts.
- Encryption: AES-256 at rest; TLS 1.2+ (preferably 1.3) in transit; enable BitLocker or equivalent.
- Screen-lock when unattended

- Use only approved cloud/storage services compliant with UK GDPR.
- Maintain patching, anti-malware, firewalls, and logging/monitoring aligned to risk.

11.3 Mobile & Remote

- Use organisation-approved devices with encryption, password/PIN, and remote-wipe.
- Minimise personal data on portable devices.
- Do not use unsecured public Wi-Fi for confidential data.

11.4 Email & Electronic Communications (including communications via Tapestry)

- Treat email as formal correspondence; legal status equals written letters.
- Do not email confidential/sensitive data externally without encryption (Outlook message encryption/Egress).
- Use TLS v1.2+, DMARC/DKIM/SPF, MTA-STS, and inbound DMARC enforcement; monitor reports.
- Validate recipients; avoid personal accounts/messaging apps for work data.
- Be vigilant against phishing/BEC; follow NCSC guidance; report suspicious emails immediately.

Email Etiquette & Rules

- Professional tone; clear and concise; avoid slang/jargon
- Use “Reply All” only when necessary
- Do not forward chain emails
- Minimise CC/BCC
- Use encryption for confidential content
- Use Outlook/Egress when sending outside the Foundation
- Follow NCSC guidance on identifying/reporting phishing.

11.5 Removable Media & Restrictions

- No unencrypted removable media; memory sticks are not permitted unless encrypted and expressly approved.
- DVD/external drives disabled unless authorised.

11.6 Data Removal Log & Off-site Handling

- Avoid transporting personal data off-site unless necessary
- Record any removal on the data removal log
- Keep physical files in locked storage
- Never leave in homes/cars overnight
- Discuss risks in supervision.

12. Records & Documentation

- Factual, relevant, accurate, and timely records; regular review.
- Maintain individual case files (e.g., EHM/Tapestry/Employment Hero/secure platforms) and operational records (attendance, programmes, incidents, medication, H&S, training, finance, insurance, DBS).
- Attendance registers marked on arrival and taken during evacuations.

13. Information Sharing

- Share only where lawful, necessary, and proportionate; record rationale.
- Use Information Sharing Agreements/DPAs with partners/processors (e.g., local authority, NHS, schools).
- Safeguarding information is shared per statutory guidance - even without consent - where a child is at risk of harm.
- Use secure channels: encrypted email (Outlook/Egress), secure portals; avoid phone disclosures unless verified.

14. Transfer & Exchange of Information

- Restrict transfer to the minimum necessary information.
- Encrypt in transit; avoid transfers outside the UK/EEA unless approved and safeguarded (e.g., SCCs/IDTA).
- Use signed-for/recorded delivery for confidential mail; verify recipients; keep disclosure records.

Secure Sharing by Post & Telephone

- Post:
    - verify recipient
    - use inner envelope marked “Private and Confidential To be opened by Addressee Only” inside a plain outer envelope
    - use signed-for/recorded delivery for confidential content
    - request receipt confirmation; record disclosure.
- Telephone:
    - verify caller via organisation switchboard
    - do not disclose if identity cannot be verified
    - do not leave detailed messages/voicemail
    - be mindful of eavesdropping
    - record disclosures.

15. Retention & Disposal

- Follow Aspire’s Data Retention Schedule (statutory/operational requirements).
- Securely delete/destroy when no longer required; for electronic files, use secure deletion preventing recovery.
- Use certified providers (e.g., ADISA-accredited) for IT asset disposal; obtain destruction certificates.

16. Subject Access Requests (SARs) & Freedom of Information (FOI)

- Handle SARs and FOI requests within statutory timeframes.
- Under DUAA, SAR searches must be “reasonable and proportionate.”
- Oversight by Organisation Strategic Lead; DPO advises and monitors compliance.

17. Individual Rights (UK GDPR)

- Right to be informed; access; rectification; erasure; restriction; portability; objection; rights related to automated decision-making/profiling (with DUAA safeguards).
- Children may exercise rights where competent; otherwise by parent/carer with parental responsibility.

18. Data Protection Impact Assessments (DPIAs)

- Conduct DPIAs for high-risk processing (new systems, online services, profiling, large-scale special category data).
- Implement mitigations; record decisions and outcomes.

19. Training & Awareness

- Induction IG/data protection training for all; annual refreshers and role-specific modules (safeguarding, IT systems).
- Include cyber security and AI-related risks awareness as relevant to email/content generation.

19. Incident Management & Breach Reporting

- Report immediately any suspected/actual breach (loss, theft, unauthorised access, accidental disclosure) to DPO/Manager.
- Assess risk; if likely to impact rights/freedoms, notify ICO within 72 hours and affected individuals where appropriate.
- Document incidents, actions, and lessons learned; apply disciplinary measures for deliberate/negligent breaches per Code of Conduct.

20. Account Lifecycle & Access Management

- New starters: accounts created on/after start date via HR-verified process; assign role based access control based on role/site; apply MFA.
- Movers: adjust access promptly; remove access to prior case folders; review privileges.
- Leavers: deactivate accounts and revoke access immediately; recover all devices/media; confirm data hand-back.

Access Control Matrix (summary):

- SMT: all files (except legally restricted where applicable)
- Early Years teams: site-specific folders
- Community Family Workers: Targeted Family Support folders
- Admin/Finance/Volunteer Coordination: operational folders excluding individual case files
- Students: site-specific; social work students may access individual case files at their site with supervisor approval

21. ICT Systems & Technical Controls (Summary)

- Centralised identity/access management; VPN/MFA for remote; server/endpoint anti-malware; firewalling; patching; logging/monitoring.
- Email via Microsoft 365 with Egress for external confidential messaging; enforce DMARC/DKIM/SPF/MTA-STS; review TLS-RPT/DMARC reports regularly.
- Group Policy/MDM to enforce encryption and restrict removable media.
- Periodic site checks by IT; event log reviews; service/process monitoring.

22. Monitoring, Audit & Review

- Regular audits of Information Governance controls, access permissions, and policy adherence.
- Report findings to SMT/Trustees; track actions to closure.
- Annual policy review or sooner if law/guidance changes or after incidents.

References (UK)

ICO: Encryption and data protection: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/encryption/encryption-and-data-protection

GOV.UK: Data (Use and Access) Act 2025 – data protection changes: https://www.gov.uk/guidance/data-use-and-access-act-2025-data-protection-and-privacy-changes

Data Protection Report: UK data protection reform (DUAA overview): https://www.dataprotectionreport.com/2025/07/uk-data-protection-reform-what-you-need-to-know-and-do/

Greenberg Traurig: DUAA key changes: https://www.gtlaw.com/en/insights/2025/6/uk-data-access-and-use-act-2025-key-changes-seek-to-streamline-privacy-compliance

GOV.UK: Securing government email: https://www.gov.uk/guidance/securing-government-email

NCSC: Phishing guidance: https://www.ncsc.gov.uk/guidance/phishing