Data Protection and GDPR Policy

United African Association

Registered Charity CIO 1192725
Unit F5B Barratt House Kingsthorpe Road Northampton NN2 6EZ
www.uaassociation.org

Policy owner	Board of Trustees
Version	1.0
Approval status	Approved by the Chair
Approval date	October 2026
Next review	October 2027
Applies to	Trustees staff volunteers contractors and relevant partners

Purpose

This policy governs UAA's handling of personal data about beneficiaries, families, donors, staff, volunteers, trustees, applicants, partners and website users.

Scope

This policy applies wherever UAA works, including Barratt House, Leicester Street Community Centre, partner venues, the foodbank and food larder, community meals, welcoming spaces, youth activities, football, swimming, wellbeing sessions, allotment work, trips, outreach, home or hospital visits, online sessions, social media and transport arranged by UAA.

Legal and good practice framework

- UK General Data Protection Regulation
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations 2003
- ICO guidance

Responsibilities

Role	Responsibility
Board of Trustees	Approves the policy, receives assurance, provides resources and remains accountable.
Chief Executive or delegated manager	Implements the policy, allocates competent leads and escalates significant matters.
Policy lead	Maintains procedures, records, training and contact details and reports themes to trustees.
Staff volunteers and contractors	Follow the policy, attend required training and report concerns promptly.

Data protection principles

- Lawfulness fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

UAA data and lawful bases

UAA processes contact details, demographic and equalities information, referral and case notes, safeguarding information, health or dietary needs, attendance, images, donor records, employment and volunteer records, and monitoring data. The responsible lead records the purpose, lawful basis and any condition for special category data before collection.

Collection and privacy information

People are told what UAA collects, why, who it may share with, how long it keeps it and how to exercise their rights. Consent is specific and withdrawable where consent is the lawful basis. Safeguarding information is not withheld from necessary sharing simply because consent is unavailable.

Security and access

- Use approved accounts and devices, strong passwords and multi-factor authentication where available.
- Do not store casework on personal devices or send sensitive information through unapproved channels.
- Lock paper files and screens, check recipients before sending and use secure transfer for sensitive information.
- Limit access by role and remove access promptly when a person leaves.

Individual rights

Requests for access, correction, deletion, restriction, objection or data portability are sent to the data protection lead and logged. UAA responds within the legal timescale and verifies identity proportionately.

Personal data breaches

1. Contain the breach and protect people from immediate harm.
2. Report it immediately to the data protection lead, preserving evidence.
3. Assess the likelihood and severity of risk to people.
4. Notify the ICO within 72 hours where required and inform affected people without undue delay where risk is high.
5. Record every breach, the assessment, action and learning.

Retention and disposal

UAA maintains a retention schedule based on purpose, safeguarding needs, employment, finance, insurance, funding and limitation periods. Records are securely deleted or destroyed when no longer required.

Processors partners and international transfers

Written terms must protect data when a supplier or partner processes it for UAA. Personal data is not transferred internationally without an approved safeguard and documented assessment.

Records and confidentiality

UAA will keep proportionate, accurate and secure records. Access is limited to people who need the information for their role. Records are retained and disposed of in line with the Data Protection and GDPR Policy and any legal, insurance or funding requirement.

Training and communication

The policy lead will include this policy in induction and arrange refresher or role-specific training where the level of risk requires it. Current procedures and reporting routes will be accessible to staff and volunteers.

Monitoring and review

The policy lead will monitor incidents, complaints, near misses, audit findings and feedback. The Board will review this policy at least annually and sooner after a serious incident, material legal or operational change, significant complaint or identified control failure.

Related UAA policies

- Child Safeguarding Policy
- Adult Safeguarding Policy
- Incident and Serious Incident Reporting Policy
- Information Advice and Signposting Boundaries Policy
- Social media rules within the Code of Conduct Policy

Approval

Approved by the Chair



Raymond
Chair of UAA
Approval date: October 2026
Next review date: October 2027