REACHING ALL PEOPLE TRUST CIC

Company No. 10349786

GDPR & DATA PROTECTION POLICY

Document owner	Reaching All People Trust CIC
Public-facing delivery platform	RAP Academy®
Version	1.0
Effective date	1 September 2026
Review date	September 2027, or earlier where required
Classification	Public
General contact	info@rapacademy.org

Policy status: RAP Trust's 2026 Governance Handbook identifies a GDPR and Data Protection Policy as part of the organisational policy framework. As the complete substantive source text was not recoverable from the supplied handbook, this document is a controlled 2026 policy construction rather than a verbatim reconstruction. It is designed for the legal framework in force at its effective date.

1. Statement of Commitment

Reaching All People Trust CIC is committed to handling personal information lawfully, fairly, transparently and securely. Data protection is treated as an organisational governance responsibility and is embedded within safeguarding, programme delivery, monitoring and evaluation, partnership working, workforce management and digital engagement.

2. Purpose

This policy establishes how RAP Trust will govern the collection, use, sharing, storage, protection and disposal of personal information and how it will support individuals to exercise their information rights.

- Protect the rights and freedoms of people whose information RAP Trust handles.
- Provide a consistent framework for lawful and accountable processing.
- Support safe information sharing where safeguarding, delivery or legitimate organisational functions require it.
- Ensure higher-risk processing receives appropriate scrutiny.
- Provide a clear route for data-protection concerns and complaints.

3. Scope

This policy applies to personal information processed by or on behalf of Reaching All People Trust CIC across its organisational and delivery activities. RAP Academy®, RAP Mentors® and associated programme identities operate within the wider Reaching All People Trust CIC framework. It applies to trustees, staff, volunteers, contractors and others processing personal information for RAP Trust.

- Participant and referral information.
- Children's and young people's information.
- Safeguarding and risk information.
- Staff, trustee, volunteer and contractor information.
- Commissioner, partner and professional-contact information.
- Programme monitoring, evaluation and outcome information.
- Website, enquiry and digital-communication information.
- Photographs, video, audio and other media where personal information is involved.

4. Legal and Regulatory Framework

This policy is intended to operate consistently with the UK data-protection framework applicable at the effective date.

- UK General Data Protection Regulation (UK GDPR), as amended.
- Data Protection Act 2018, as amended.
- Data (Use and Access) Act 2025 (DUAA), whose data-protection provisions are in force.
- Privacy and Electronic Communications Regulations (PECR), where applicable.
- Current guidance issued by the UK's data-protection regulator, the Information Commissioner's Office (ICO).

5. Data Protection Principles

RAP Trust will apply the core data-protection principles to its processing activities.

- Lawfulness, fairness and transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality (security).
- Accountability.

6. Lawful Bases

Before processing personal information, RAP Trust must identify and document an appropriate lawful basis under the UK GDPR. Consent will be used only where it is genuinely appropriate and can meet the legal standard. Other lawful bases may be more appropriate for contractual, legal, safeguarding, employment, legitimate organisational or public-interest functions depending on the circumstances.

7. Special Category and Criminal Offence Data

RAP Trust may encounter information requiring enhanced protection, including health information, racial or ethnic origin, religious or philosophical beliefs, sexual orientation, biometric information used for identification, and information concerning criminal allegations, convictions or offences. Processing must have an Article 6 lawful basis and, where required, an additional Article 9 condition or an appropriate condition under the Data Protection Act 2018. Criminal-offence data must be handled only where the legal requirements for that processing are met.

8. Children's and Young People's Information

Because RAP Trust works with children and young people, their information requires particular care. Processing should be transparent and understandable, proportionate to the purpose, and designed with children's interests and rights in mind. Data protection by design and default must consider the higher-protection requirements applicable to children's personal information.

9. Safeguarding Information

Data protection law does not prevent necessary safeguarding information sharing. Where RAP Trust processes or shares information to protect a child or an individual at risk, staff must consider necessity, proportionality, lawful basis, applicable special-category or criminal-offence conditions, accuracy, security and appropriate recording. Safeguarding decisions must not be delayed merely because information is sensitive.

10. Transparency and Privacy Information

RAP Trust will provide appropriate privacy information explaining, in clear language, who is handling personal information, why it is used, relevant lawful bases, who it may be shared with, how long it may be retained or how retention is determined, individual rights, and how to raise a concern. Separate privacy notices may be required for different groups or processing activities.

11. Data Minimisation and Accuracy

Only personal information reasonably necessary for a defined purpose should be collected or used. Information should be adequate, relevant and limited to what is necessary. Reasonable steps must be taken to keep information accurate and, where appropriate, up to date.

12. Retention and Secure Disposal

Personal information must not be retained indefinitely without justification. RAP Trust will determine retention by reference to purpose, legal and contractual requirements, safeguarding considerations, limitation periods, commissioning requirements and organisational need. A detailed retention schedule should be maintained separately where required. When information no longer needs to be retained, it must be securely deleted, destroyed or anonymised as appropriate.

13. Information Security

RAP Trust will use proportionate technical and organisational measures to protect personal information against unauthorised or unlawful access, loss, destruction, alteration or disclosure. Access should be limited according to role and legitimate need. Staff must use approved organisational arrangements for handling sensitive information and report suspected security incidents promptly.

14. Information Sharing and Partnership Working

Personal information may be shared with commissioners, statutory agencies, education, health, justice, safeguarding or community partners where there is a legitimate and lawful reason. RAP Trust will consider the purpose, lawful basis, necessity, proportionality, security and transparency of sharing. Appropriate agreements or contractual provisions should be used where required.

15. Controllers, Processors and Suppliers

Where another organisation processes personal information on RAP Trust's behalf, appropriate due diligence and legally compliant contractual arrangements must be used. Where RAP Trust and another organisation determine purposes and means together, the parties should clarify their respective responsibilities. Organisational labels must not be used as a substitute for determining the actual legal relationship.

16. Individual Rights

RAP Trust will facilitate applicable rights under data-protection law, including rights relating to access, rectification, erasure, restriction, objection, portability where applicable, and safeguards relating to solely automated decisions where relevant. Rights are not absolute and requests will be assessed according to the law and circumstances.

17. Subject Access Requests

Requests for access to personal information must be recognised and handled promptly, including requests that do not use the phrase 'subject access request'. Identity may be verified where reasonably necessary. RAP Trust will respond within the statutory timeframe applicable to the request and may extend that timeframe only where the law permits. Third-party information, safeguarding considerations and applicable exemptions must be assessed carefully.

18. Data Protection Complaints

RAP Trust will provide an accessible route for individuals to complain about how their personal information has been handled. Complaints may be sent to **info@rapacademy.org** unless a more specific approved route is provided. RAP Trust will acknowledge a data-protection complaint within 30 days, investigate it without undue delay, keep the complainant appropriately informed and communicate the outcome without undue delay. Records of complaints and responses should be maintained.

19. Personal Data Breaches

A personal data breach includes a security incident leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information. Suspected breaches must be escalated promptly for assessment. RAP Trust will document relevant breaches and, where the legal threshold is met, notify the ICO and affected individuals within the applicable statutory requirements.

20. Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) must be considered before processing that is likely to result in high risk to people's rights and freedoms. This is particularly important for new technologies, systematic monitoring, large-scale sensitive processing or other higher-risk activities. DPIAs should identify purpose, necessity, proportionality, risks and mitigating measures.

21. Data Protection by Design and Default

Privacy and data protection should be considered at the start of new programmes, systems, forms, partnerships and data uses rather than added retrospectively. Default settings and processes should limit personal information to what is necessary for the defined purpose. Children's higher-protection matters must be considered where relevant.

22. Media, Images and Digital Communications

Photographs, video, audio, testimonials and other identifiable media are personal information where an individual can be identified. RAP Trust must identify an appropriate lawful basis, provide suitable transparency information, respect safeguarding considerations and apply particular care to children's information. Marketing communications and electronic communications must also comply with PECR where applicable.

23. Monitoring, Evaluation and Research

Programme monitoring and evaluation should use only information necessary for defined purposes. Wherever practicable, reporting to commissioners, partners or the public should use aggregated or anonymised information. Where identifiable, special-category or criminal-offence information is required, the relevant legal conditions and safeguards must be documented.

24. International Transfers

Personal information must not be transferred outside the UK unless the applicable UK data-protection requirements for international transfers are met. Before introducing systems or suppliers involving overseas transfers, RAP Trust must identify the transfer mechanism and appropriate safeguards.

25. Training and Responsibilities

Anyone handling personal information for RAP Trust is responsible for following this policy, maintaining confidentiality, completing appropriate training and reporting concerns. Leadership is responsible for ensuring proportionate governance, policies, training, contractual controls and oversight. This policy does not state that RAP Trust has appointed a statutory Data Protection Officer; any such appointment must be formally determined and recorded if required.

26. Accountability and Documentation

RAP Trust will maintain documentation proportionate to its processing and legal obligations. This may include privacy notices, records of processing, lawful-basis decisions, data-sharing arrangements, processor contracts, DPIAs, breach records, complaint records and retention arrangements. Documentation should demonstrate that data-protection decisions are considered rather than assumed.

27. Policy Review

This policy will be reviewed at least annually and earlier following significant legislative or regulatory change, ICO guidance materially affecting RAP Trust, a significant personal-data breach, identified organisational learning or material change to RAP Trust's processing activities. The planned annual review date is September 2027.

Document Control

Policy	GDPR & Data Protection Policy
Organisation	Reaching All People Trust CIC
Company number	10349786
Version	1.0
Effective date	1 September 2026
Review date	September 2027 or earlier if triggered
Classification	Public
General contact	info@rapacademy.org

Related governance: Safeguarding and Child Protection; Privacy Notices; Safer Recruitment; Monitoring and Evaluation; Whistleblowing; Risk Assessment. Further cross-references should be maintained as the standalone governance suite is completed.

Implementation note: This policy deliberately does not invent a Data Protection Officer, fixed retention periods, named software systems, cloud providers or technical controls that have not been verified. Those operational details should be documented separately where applicable.