



Record of Processing Activities (ROPA)

Below is our Record of Processing Activities (ROPA) tailored for Autism Mentors Ltd, aligned with UK GDPR (Article 30) requirements and consistent with your policies.

We have adapted this into a spreadsheet on our cvvc database for ongoing use.

#	Purpose of Processing	Data Subjects / Categories	Types / Categories of Personal Data	Recipients / Categories of Recipients	International Transfers (if any)	Retention Period / Erasure Schedule	Technical & Organisational Security Measures	Lawful Basis (incl. special category condition)	Notes / Comments
1	Provision of mentoring & care support to clients	Clients (children, young people, adults)	Identifiers (name, DOB, address), contact details, health & neurodiversity / SEN information,	Internal staff, local authorities, schools, health professionals, social care	None / UK-based system only (cloud server within UK or approved jurisdiction)	6 years after end of service, unless statute demands longer	Encrypted storage, restricted access, role-based permissions, secure physical files, passwords	Contract / Legitimate interest / Consent (for health data) + appropriate condition	Client consent forms, safeguarding consents, DPIA status

			educational reports, behavioural / incident records, safeguarding history				ord protection, regular backups	Schedule 1 DPA 2018 for special category data	
2	Safeguarding and protection of individuals	Clients, families, staff, volunteers	Safeguarding disclosures, incident reports, investigative records, risk assessments	Local authority, MASH, police, LADO, regulators	As above	At least 6–25 years (or in line with statutory guidance)	Secure access, anonymisation when possible, audit logging, secure deletion when no longer needed	Legal obligation / Vital interests / Public task	Some records may need to be held longer per local authority guidance
3	Recruitment, HR & staff management	Applications, employees, contractors, volunteers	Application forms, CVs, references, DBS checks, training	Internal HR team, DBS/enhanced check service, regulators	None	6 years post-employment or per internal HR policy	Access control, secure HR system, encryption, regular	Contract / Legal obligation	Must handle DBS data especially carefully

			records, supervision notes, performance records	ors (if required)			review & deletion	(special rules)	
4	Training & professional development	Staff, contractors, volunteers	Training records, CPD evidence, qualifications, certificates	Internal management, training providers, auditing bodies	None	Duration of employment plus 6 years	Controlled access, encrypted backup, role restrictions	Legitimate interest / Contractual obligation	Link to supervision & performance reviews
5	Communications, scheduling, operational administration	Clients, staff, families	Contact details, email correspondence, session notes (non-sensitive)	Internal staff, scheduling system providers	None (or standard cloud providers)	3 years after last contact or as needed	Encrypted systems, secure email, two-factor authentication	Legitimate interest / Contract	Segment data to limit exposure of sensitive parts
6	Data protection, complaints, internal	Clients, staff	Data breach records, complaints	Directors, legal advisors, ICO (if	None	7 years or as required by statute	Audit trails, restricted files, encrypted	Legal obligation / Legitimate interest	Link to related policies (data breach,

govern
ance

files,
audit
logs

request
ed)

ed
storage

grievan
ce)

Additional Notes & Considerations

- Controller / Data Protection Lead
 - Controller: Autism Mentors Ltd
 - Data Protection Lead / Contact: Michelle Wray (DSL)
 - Address, email, and telephone should be documented in full in your master ROPA record.
- Special / Sensitive Categories

Many of your processing activities involve special category data (health, disability, behavioural, safeguarding). You must specify the appropriate condition under Schedule 1 of the Data Protection Act 2018 for each processing activity (e.g. “processing is necessary for the exercise of legal obligations in relation to safeguarding,” or “explicit consent”).
- Processors and Third Parties

If you use external processors (e.g. cloud storage, HR platform, scheduling software), document:

 - The processor name and contact details
 - The categories of processing they perform
 - Assurance they meet UK GDPR obligations
- Updating the ROPA
 - Treat it as a living document — review and update it whenever there’s a new processing activity or when systems / contracts change.
 - Assign clear responsibility for maintaining and auditing the ROPA.

- Exemptions for Small Organisations

Under UK GDPR, organisations with fewer than 250 employees may be exempt from maintaining full processing records unless the processing is regular, involves special categories, or is likely to pose risk to data subjects. But because you handle health and safeguarding data, you should maintain full ROPA.

- Retention & Disposal

Ensure your ROPA links to your data retention and disposal policy. For example, client files: how and when they are deleted, archived, or anonymised.

- Security Measures Description

Your ROPA should include a general description of security measures (encryption, restricted access, backups, secure physical storage) to satisfy Article 30 requirements.

- Making It Available

You must make the ROPA available on request to the ICO.

If you like, I can convert this into a fillable Excel template customized for Autism Mentors Ltd, so you and your team can populate and maintain it easily. Would you like me to produce that for you now?