Acorn Autism Specialists

Diagnosis | Independence | Well-being

UK GDPR Policy

Policy & Procedure

Document reference	AAS-POL-007
Version	v2026.1
Issue / review date	April 2026
Next scheduled review	April 2027
Policy lead	Data Protection Lead
Statutory / regulatory basis	UK GDPR; DPA 2018
Legal status	MANDATORY – UK GDPR / DPA 2018

Approved by the Directors of Acorn Autism Specialists

Legislative & regulatory framework

- UK GDPR
- Data Protection Act 2018
- Data Protection and Digital Information Act 2025 (as enacted)
- ICO Accountability Framework
- EHRC guidance on equality data (where relevant)

1 Purpose

This policy operationalises the UK GDPR within Acorn Autism Specialists and sits beneath the Data Protection Policy. It is the working-level rulebook for staff.

2 Key Definitions

- **Personal data:** information relating to an identified or identifiable living person.
- **Special category data:** racial/ethnic origin, political opinions, religious beliefs, trade-union membership, genetic, biometric, health, sex life, sexual orientation data.
- **Processing:** any operation performed on personal data, including collecting, storing, using, disclosing or deleting.
- **Data Subject:** a living individual whose personal data we process.

3 How we meet Accountability

- Documented policies and procedures
- A ROPA maintained under Article 30
- DPIAs for high-risk processing
- Article 28 contracts with all processors
- Mandatory annual data-protection training
- Information-security controls documented in the ISMS
- Regular internal audit against the ICO Accountability Framework

4 Data Subject Rights Requests (DSARs)

Requests may be made verbally or in writing and do not have to cite the UK GDPR. All staff must recognise a request and pass it to the DPL within one working day. Acorn responds within one calendar month, extendable by up to two further months for complex or numerous requests.

5 Direct Marketing & PECR

Electronic marketing to individuals is only carried out with explicit opt-in consent (or the limited "soft opt-in" for existing clients). All marketing offers a clear one-click unsubscribe.

6 Website Cookies

Acorn's website uses only strictly necessary cookies by default; any analytics or marketing cookies require explicit opt-in consent via the cookie banner, in line with PECR Reg 6 and ICO guidance.

7 Training & Awareness

All staff complete a mandatory data-protection e-learning module on induction and refresh it at least annually. Role-specific training is provided to clinicians and admin staff.

8 Roles & Responsibilities

Role	Responsibility
Data Protection Lead	GDPR compliance, ROPA, DPIAs, rights requests, breach response, training.
Managers	Embed DP into team processes; escalate risks.
Staff	Handle personal data in line with the policy; complete training; report breaches immediately.

9 Breach of Policy

Non-compliance may result in disciplinary action and regulatory action by the ICO.

10 Monitoring & Review

This policy will be reviewed at least annually, or sooner if legislation, regulatory guidance, or best practice changes, by the Policy Lead in conjunction with the Directors.

11 Related Documents

- Data Protection Policy
- Privacy Policy

- Client Privacy Notice
- Information Security Breach Policy

Approval & Sign-off

Approved by	Board of Directors, Acorn Autism Specialists
Date approved	April 2026
Next review	April 2027