



Acorn Autism Specialists

Diagnosis | Independence | Well-being

Data Protection Policy

Policy & Procedure

Document reference	AAS-POL-006
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; PECR 2003
Legal status	MANDATORY – UK GDPR / Data Protection Act 2018

Approved by the Directors of Acorn Autism Specialists

Legislative & regulatory framework

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations 2003 (PECR)
- Freedom of Information Act 2000 (where applicable)
- Data Protection and Digital Information Act 2025 (as enacted)
- Common-law duty of confidentiality
- Caldicott Principles (2020 refresh)
- NHS Data Security and Protection Toolkit (where relevant)
- Human Rights Act 1998 – Article 8

1 Statement

Acorn Autism Specialists (“Acorn”, “we”) is a data controller registered with the Information Commissioner’s Office (ICO). We are committed to processing personal data lawfully, fairly and transparently, and to upholding the rights of our clients and staff.

2 Scope

This policy covers all personal data processed by Acorn in any format (paper, electronic, verbal, imaging) and applies to all staff, contractors, directors, volunteers and processors.

3 Data Protection Principles (Article 5)

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

4 Lawful bases we rely on

- **Article 6(1)(b) Contract:** to deliver assessments to a client.
- **Article 6(1)(c) Legal obligation:** e.g., safeguarding, regulatory reporting, accounting.
- **Article 6(1)(f) Legitimate interests:** for limited administrative purposes following a Legitimate Interests Assessment.
- **Article 9(2)(h) Special category:** provision of health or social care.

-
- **Article 9(2)(b):** employment, social security and social protection.
 - **Article 9(2)(a) Explicit consent:** for ancillary or optional processing (e.g., recording, research).

5 Individual Rights

-
- Right to be informed (Articles 13–14)
 - Right of access (Article 15)
 - Right to rectification (Article 16)
 - Right to erasure (Article 17) – subject to our legal and regulatory retention duties
 - Right to restrict processing (Article 18)
 - Right to data portability (Article 20)
 - Right to object (Article 21)
 - Rights in relation to automated decision-making (Article 22)

6 Roles

Acorn has appointed a Data Protection Lead (DPL) who acts as the single point of contact for data-protection matters. Where our processing meets the Article 37 thresholds we will appoint a Data Protection Officer (DPO). All staff are accountable for the personal data they handle.

7 Data Protection by Design & Default

New projects, systems and processes are subject to a Data Protection Impact Assessment (DPIA) where they are likely to result in high risk to data subjects. Privacy is built in at the design stage, not bolted on.

8 International Transfers

Where we transfer personal data outside the UK we use UK adequacy regulations, the UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU SCCs, supported by a Transfer Risk Assessment.

9 Record of Processing Activities (ROPA)

Acorn maintains a ROPA under Article 30, reviewed at least annually by the DPL.

10 Retention & Disposal

Personal data is retained in line with the Records Management Policy and securely destroyed when no longer needed.

11 Personal Data Breaches

Any suspected personal-data breach must be reported immediately to the DPL in line with the Information Security Breach Policy. The DPL determines whether notification to the ICO within 72 hours and/or to affected individuals is required.

12 Roles & Responsibilities

Role	Responsibility
Directors	Ultimate accountability for data-protection compliance.
Data Protection Lead	Day-to-day compliance, ROPA, DPIAs, rights requests, breach management, training.
All staff	Follow the policy; complete annual DP training; report concerns and breaches immediately.
Processors	Process only on documented instructions under a written Article 28 contract.

13 Breach of Policy

Failure to comply may result in disciplinary action, regulatory enforcement by the ICO (including fines up to £17.5m or 4% of global turnover), civil claims and reputational damage.

14 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.

15 Related Documents

- GDPR Policy
- Data Protection Procedure
- Privacy Policy
- Client Privacy Notice
- Records Management Policy
- Information Security Breach Policy

Approval & Sign-off

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