



Chichester Forest Schools – Data Protection Policy (UK GDPR Compliant (2026)

Version: 3.1

Issued: 12 Feb 2026

Next Review: 12 Feb 2027

1. Purpose

Chichester Forest Schools is committed to protecting the privacy, security, and rights of all individuals whose personal data we process. This policy explains how we collect, use, store, and share personal information in accordance with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- ICO guidance for schools and education providers

We recognise that children's data requires additional protection due to their vulnerability and limited understanding of privacy rights.

2. Data Protection Officer

Rachel Maynard, CEO

Email: rachel@chichesterforestschoools.com

The DPO oversees compliance, advises on data protection matters, and acts as the point of contact for data subjects and the ICO.

3. Categories of Personal Data We Collect

We collect only the data necessary for our educational, safeguarding, and operational purposes.

3.1 Identifiers

- Name, address, phone number, email
- Date of birth

- National Insurance number

3.2 Special Category Data

Processed only where strictly necessary:

- Medical information
- Mental health details
- Safeguarding information
- SEND/EHCP information

3.3 Employee Data

- Payroll and HR records
- DBS checks
- Qualifications and training
- Employment history

3.4 Referrer and School-Provided Data

- Risk assessments
- EHCPs
- Behaviour or safeguarding reports

4. Purposes of Processing

We process personal data for the following purposes:

4.1 Education and Programme Delivery

- Planning and delivering Forest School sessions
- Supporting learning, wellbeing, and personal development

4.2 Safeguarding and Welfare

- Identifying and supporting children at risk
- Liaising with schools, social care, and safeguarding partners

4.3 SEND and Additional Needs

- Providing appropriate support
- Meeting statutory duties relating to EHCPs

4.4 Administration and Communication

- Booking systems
- Session updates
- Emergency contact

4.5 Legal and Statutory Requirements

- Incident reporting
- Health and safety compliance
- Employment law obligations

4.6 Marketing and Promotion

- Newsletters
- Photographs
- Social media content (with consent)

5. Lawful Bases for Processing

We rely on the following lawful bases under UK GDPR:

5.1 Public Task

For activities necessary to deliver education, safeguarding, SEND support, and operational functions.

5.2 Legal Obligation

For statutory reporting, safeguarding disclosures, employment law, and health and safety.

5.3 Consent

Used only when strictly appropriate:

- Newsletters
- Photographs
- Zoom recordings

Consent can be withdrawn at any time by contacting the DPO.

5.4 Legitimate Interests

For limited activities such as:

- Administrative updates
- Session summaries
- Non-essential marketing

A documented Legitimate Interest Assessment (LIA) is maintained and available on request.

6. Special Category Data – Article 9 Conditions

We process special category data under:

- Article 9(2)(g): Substantial public interest (safeguarding, child protection)
- Article 9(2)(h): Health or social care provision
- Article 9(2)(c): Vital interests (where a child is at risk)
- Article 9(2)(a): Explicit consent (only where appropriate)

7. Children's Data

We recognise that children require enhanced protection. Therefore:

- We minimise the data collected
- We ensure data is shared only when necessary for safeguarding or educational purposes

8. Data Sharing and Third-Party Processors

We share data only when necessary and proportionate.

8.1 Third-Party Processors

We use GDPR-compliant processors including:

- Mailchimp
- Bookwhen
- Eventbrite
- Zoom
- WhatsApp
- Microsoft Office
- Facebook, Instagram, LinkedIn
- Indeed
- Linktree

All processors have signed Data Processing Agreements.

8.2 International Data Transfers

Some processors may transfer data outside the UK.

Where this occurs, we ensure appropriate safeguards such as:

- UK International Data Transfer Agreement (IDTA)
- Standard Contractual Clauses (SCCs)
- Adequacy decisions

Details are available on request.

9. Retention Periods

We retain data only as long as necessary:

- Service user data: up to 3 years unless required longer by law
- Employee records: in line with statutory requirements

A detailed retention schedule is available on request.

10. Data Accuracy and Minimisation

We ensure that personal data is:

- Adequate
- Relevant
- Limited to what is necessary
- Kept accurate and up to date

Individuals may request corrections at any time.

11. Security Measures

We protect data through:

- Secure digital systems with restricted access
- Encrypted storage where appropriate
- Shredding of paper records
- Regular review of security practices

12. Automated Decision-Making

We do not use automated decision-making or profiling.

If this changes, we will update this policy and notify individuals.

13. Your Rights

Under UK GDPR, individuals have the right to:

- Access their data
- Rectify inaccurate data
- Request erasure
- Restrict processing
- Object to processing
- Data portability
- Withdraw consent
- Lodge a complaint with the ICO

Subject Access Requests (SARs)

Submit SARs to the DPO.

We respond within one month.

14. Photographs and Zoom Recordings

- Used only with consent
- Names are never published
- Zoom recordings are used only for sharing and record-keeping

15. Safeguarding

We may share personal data without consent where legally required to protect a child, in line with our Safeguarding Policy.

16. Complaints

If you have concerns about how we handle your data:

1. Contact the DPO
2. If unresolved, escalate to the CEO or governing body
3. You may then contact the ICO

17. Review and Updates

This policy is reviewed annually or sooner if required by law or operational changes.

Accepted by the Directors Board 12.02.2026

Review date 12.02.2027