





THE ORCHARD SCHOOL

GDPR, Data Protection, Document Control and Data Retention Policy

Draft:	December 2025
Ratified:	December 2025
Review:	September 2026
Chair of Governors:	
Headteacher:	

Ethos of The Orchard School

At The Orchard School, Everyone Matters, Everyone Cares. Our ethos is rooted in the belief that every child has the potential to grow, thrive, and succeed when provided with the right environment, relationships, and support. The Orchard Way guides everything we do, ensuring that our approach is therapeutic, inclusive, and centred on understanding behaviour as communication. We are committed to nurturing the social, emotional, and mental health (SEMH) needs of our pupils, recognising their unique challenges while celebrating their individuality. Through strong relationships and a culture of care, we create a school where every pupil feels safe, valued, and empowered to reach their full potential.

Principles of Our Ethos:

1. **Respect for the Individual:** Every pupil deserves respect, dignity, and the opportunity to be heard.
2. **Relationships at the Heart of Learning:** Positive, trusting relationships form the foundation of our work.
3. **Equity and Inclusion:** We ensure all pupils have access to the support they need to succeed.
4. **Therapeutic and Nurturing Approaches:** We integrate therapeutic strategies to promote resilience.
5. **High Expectations with Compassion:** Balancing aspirations with understanding and personalisation.
6. **Collaboration with Stakeholders:** Families, carers, and agencies work together to support pupils.
7. **A Safe and Predictable Environment:** Structure and boundaries foster trust and confidence.
8. **Restorative Practices:** Addressing conflicts through understanding, accountability, and growth.

Mission Statement

At The Orchard School, Everyone Matters, Everyone Cares. Our ethos is rooted in the belief that every child has the potential to grow, thrive, and succeed when provided with the right environment, relationships, and support. The Orchard Way guides everything we do, ensuring that our approach is therapeutic, inclusive, and centred on understanding behaviour as communication. We are committed to nurturing the social, emotional, and mental health (SEMH) needs of our pupils, recognising their unique challenges while celebrating their individuality. Through strong relationships and a culture of care, we create a school where every pupil feels safe, valued, and empowered to reach their full potential.

1. Purpose

1.1 This policy sets out how The Orchard School manages personal data, records and documented information in a lawful, secure and transparent manner.

1.2 It brings together:

- UK GDPR compliance
- Data protection responsibilities
- Document control expectations
- Statutory data retention requirements

1.3 The policy ensures that information, particularly **safeguarding and child protection data**, is:

- Collected for clear and lawful purposes
- Stored securely
- Accessed only by authorised staff
- Retained appropriately
- Disposed of safely

1.4 This policy supports safeguarding practice by ensuring information governance protects pupils, staff and families from harm, misuse or inappropriate disclosure.

2. Scope

2.1 This policy applies to all personal and sensitive data held by the school, including:

- Pupil, parent and carer information
- Safeguarding and child protection records
- SEN and EHCP documentation
- Staff and personnel records
- Governance and operational records

2.2 It applies to:

- Paper records
- Electronic systems
- Cloud-based platforms
- Backup and archive systems

2.3 This policy applies to all staff, governors, volunteers, contractors and visitors who handle school information.

3. Key Definitions

- **Personal Data:** Information relating to an identifiable individual
- **Special Category Data:** Includes safeguarding, health, SEN, ethnicity and biometric data
- **Data Controller:** The Orchard School
- **Data Processor:** Organisations processing data on behalf of the school
- **Data Breach:** Any incident leading to loss, unauthorised access or disclosure of personal data

4. Roles and Responsibilities

4.1 Governing Body

- Approves this policy and reviews its effectiveness
- Ensures statutory data protection compliance
- Receives assurance on safeguarding information governance

4.2 Headteacher

- Holds overall accountability for data protection
- Ensures systems, staffing and training support compliance
- Makes final decisions on complex data protection matters

4.3 Data Protection Officer (DPO)

- Provides independent advice on GDPR compliance
- Monitors data protection practices
- Advises on data breaches and Subject Access Requests
- Acts as liaison with the Information Commissioner's Office (ICO)

4.4 Designated Safeguarding Lead (DSL)

- Oversees safeguarding record management
- Controls access to child protection files
- Ensures safeguarding data is shared lawfully and proportionately
- Authorises transfer of safeguarding records to new settings

4.5 All Staff

- Follow this policy and related procedures
- Complete mandatory data protection and safeguarding training
- Report concerns or breaches immediately

5. GDPR Principles

The Orchard School processes data in accordance with the UK GDPR principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

The school demonstrates **accountability** by documenting decisions, training staff and auditing practice.

6. Lawful Basis for Processing (Expanded)

6.1 The Orchard School processes personal data where there is a clear lawful basis, including:

- Compliance with legal obligations
- Performance of a public task in education and safeguarding
- Protection of vital interests
- Employment and contractual requirements

6.2 Safeguarding, SEN and child protection information is processed under:

- UK GDPR Article 6 (legal obligation and public task)
- UK GDPR Article 9 (substantial public interest and safeguarding of children)

6.3 Consent is **not relied upon** for safeguarding data, as doing so could place children at risk.

7. Document Control

7.1 All controlled documents:

- Have a named owner
- Are version controlled
- Are reviewed annually or sooner if required

7.2 Electronic versions held on the school system are the authoritative version.

7.3 Printed documents are considered uncontrolled and must be used with caution.

8. Secure Storage and Access

8.1 Physical Records

- Stored in locked cabinets or secure rooms
- Access limited to authorised personnel

8.2 Digital Records

- Stored on secure, password-protected systems
- Access controlled by user roles
- Systems protected by appropriate cyber security measures

8.3 Safeguarding Records

- Stored separately from main pupil files
- Access restricted to the DSL team and senior leaders
- Never removed from site unless authorised

9. Data Retention

9.1 The school retains information only for as long as necessary to meet legal, safeguarding and operational requirements.

9.2 Staff Records

- Personnel files: 6 years after employment ends
- Payroll and tax records: 6 years
- Occupational health records: 6 years
- Accident and incident records: 6 years

9.3 Pupil Records

- Pupil file: Until age 25

- Safeguarding records: Until at least age 25
- SEN records: Until age 30
- Attendance records: 3 years
- Exclusion records: 6 years after leaving

9.4 Retention decisions involving safeguarding are overseen by the DSL in consultation with SLT.

10. Secure Disposal

10.1 Paper records are disposed of through:

- Cross-cut shredding
- Approved confidential waste services

10.2 Digital records are:

- Permanently deleted
- Removed from backups where appropriate

10.3 Disposal is authorised and recorded by a senior leader.

11. Data Subject Rights (Expanded)

11.1 Individuals have the right to:

- Access their personal data
- Request correction of inaccurate data
- Request erasure where lawful
- Restrict or object to processing
- Lodge a complaint with the ICO

11.2 Requests must be made in writing.

11.3 The school responds within one calendar month.

11.4 Safeguarding and third-party exemptions are applied where disclosure could cause harm.

12. Subject Access Requests (SARs)

12.1 SARs are coordinated by the Headteacher with advice from the DPO.

12.2 Safeguarding information is reviewed carefully to:

- Protect children from harm
- Prevent disclosure of third-party data
- Comply with KCSIE guidance

12.3 Decisions are documented to demonstrate accountability.

13. Information Sharing (Expanded)

13.1 Information is shared only where it is:

- Lawful
- Necessary
- Proportionate
- Relevant to purpose

13.2 Safeguarding information may be shared without consent where there is a risk of harm.

13.3 All information sharing decisions are recorded.

14. Data Breach Management (Expanded)

14.1 A data breach includes:

- Loss of data
- Unauthorised access
- Incorrect disclosure
- Cyber incidents

14.2 All breaches must be reported immediately to the Headteacher and DPO.

14.3 The school will:

- Contain the breach
- Assess risk
- Notify the ICO within 72 hours where required
- Inform affected individuals if appropriate

14.4 All breaches and near misses are logged and reviewed.

15. Training and Awareness

15.1 All staff receive:

- Annual data protection training
- Safeguarding and confidentiality updates

15.2 DSLs and senior leaders receive enhanced training.

16. Monitoring and Compliance

16.1 Compliance is monitored through:

- Annual audits
- Safeguarding reviews
- Policy evaluations
- Incident analysis

16.2 Breaches of this policy may result in disciplinary action.

17. Policy Review

17.1 This policy is reviewed annually or sooner if:

- Legislation changes
- Safeguarding guidance is updated
- A significant breach occurs