GDPR and Data Protection Policy (inc. Biometrics)

Policy Document	GDPR and Data Protection Policy
Publication Date	September 2025
Review Date	September 2026
Executive Headteacher	Jo Anderson

This policy is written so it complies with the Independent School Standards and is taken from the National Curriculum and Ofsted framework.

Equality, Community, Growth
The Oaks
Independent Primary School

The Oaks – GDPR and Data Protection Policy

Contents

The Oaks – GDPR and Data Protection Policy

1. Aims

At The Oaks, we aim to ensure that all personal data collected about staff, pupils, parents/carers, governors, visitors, and other individuals is collected, stored, and processed in accordance with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018 (DPA 2018)**.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and Guidance

This policy meets the requirements of the:

- UK GDPR
- Data Protection Act 2018
- Freedom of Information Act 2000
- Protection of Freedoms Act 2012 (particularly in relation to biometric data)
- Education (Pupil Information) (England) Regulations 2005

It is based on guidance from the **Information Commissioner's Office (ICO)**, including:

- The ICO's guidance on UK GDPR compliance
- The ICO's code of practice for subject access requests
- The ICO's code of practice on surveillance cameras and personal information

The Seven Data Protection Principles

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

People's Privacy Rights

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability

7. The right to object
8. Rights in relation to automated decision-making and profiling

---

3. Definitions

Term	Definition
Personal Data	Any information relating to an identified or identifiable individual, such as name, identification number, location data, or online identifier. It may also include physical, physiological, genetic, mental, economic, cultural, or social identity.
Special Categories of Personal Data	Personal data that is more sensitive and needs additional protection, including data about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics (used for identification), health, or sexual orientation.
Processing	Any operation performed on personal data (e.g. collecting, recording, storing, organising, using, disclosing, erasing, etc.), whether automated or manual.
Data Subject	The individual whose personal data is being processed.
Data Controller	The organisation that determines how and why personal data is processed.
Data Processor	A third party acting on behalf of the data controller.
Personal Data Breach	A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The Data Controller

Our school processes personal data relating to parents/carers, pupils, staff, governors, visitors, and others, and is therefore a **Data Controller**.

The Oaks is registered as a Data Controller with the ICO and will renew this registration annually or as required by law.

5. Roles and Responsibilities

5.1 Governing Body

The governing body has overall responsibility for ensuring that The Oaks complies with all relevant data protection obligations.

5.2 Data Protection Officer (DPO)

The DPO oversees implementation, monitors compliance, advises on policy, and acts as the first point of contact for data subjects and the ICO.
Our DPO is the **School Business Manager**, contactable through the school office.

5.3 Executive Headteacher

Acts as the Data Controller's representative on a day-to-day basis and ensures staff compliance.

5.4 All Staff

All staff must:

- Collect, store, and process personal data in accordance with this policy
- Notify the DPO of any breaches, queries, or new data-handling activities
- Seek advice if unsure about lawful processing, consent, or sharing

Failure to comply may result in disciplinary action.

6. Data Protection Principles

Personal data must be:

- Processed lawfully, fairly, and transparently
- Collected for specified, explicit, and legitimate purposes
- Adequate, relevant, and limited to what is necessary
- Accurate and kept up to date
- Stored no longer than necessary
- Processed securely

This policy outlines how we comply with these principles.

7. Collecting Personal Data

7.1 Lawfulness, Fairness and Transparency

We will only process personal data where we have a lawful basis:

- To fulfil a contract with the individual
- To comply with a legal obligation
- To protect someone's vital interests
- To perform a public task in the public interest
- For legitimate interests (unless overridden by the individual's rights)
- With explicit consent

For special category data, we meet the additional conditions set out in Article 9 of the UK GDPR.

7.2 Limitation, Minimisation and Accuracy

We collect only the data we need for specified purposes, keep it accurate, and delete it when no longer required.

7.3 Privacy Notices

We maintain privacy notices for staff, parents/carers, pupils, governors, and volunteers explaining what data we collect, why, and how it is used. These are available on our website or from the school office.

7.4 Children's Data and Online Services

Consent for online services will be sought from parents or carers for children under 13.

8. Sharing Personal Data

We may share data where:

- Required by law or safeguarding obligations
- Necessary for contractors or service providers (e.g. IT support, catering)
- Needed for emergency services or local authorities

All third parties are vetted and must provide sufficient guarantees of GDPR compliance.

Where personal data is transferred outside the **UK**, we ensure compliance with adequacy decisions or use approved safeguards, such as **International Data Transfer Agreements (IDTAs)** or **Standard Contractual Clauses (SCCs)**.

9. Subject Access Requests and Rights of Individuals

Individuals can request access to their personal data ("Subject Access Request"). Requests must be made in writing and will be responded to within one month.

The DPO manages all requests and ensures identity verification. Requests may be refused or charged only if unfounded or excessive.

Individuals also have rights to:

- Rectification
- Erasure
- Restriction
- Data portability
- Objection
- Withdraw consent
- Challenge automated decision-making

10. Parental Requests to See the Educational Record

Parents/Carers (or those with parental responsibility) have the right to free access to their child's educational record within 15 school days of a written request.

11. Photographs and Videos

We may take photographs and videos for school activities, publications, or online platforms.

Written parental consent is obtained for identifiable use. Consent may be withdrawn at any time. No additional personal data will accompany published images.

11A. Biometric Data

Where the school uses biometric systems (e.g. fingerprint or facial recognition for identification or catering), we comply with the **Protection of Freedoms Act 2012** and **UK GDPR**.

We will:

- Inform parents/carers, pupils, and staff about the use and purpose of biometric data

- Obtain written consent from parents/carers or the individual if over 18
- Provide a non-biometric alternative for anyone who objects
- Securely store and encrypt biometric data
- Delete biometric data when consent is withdrawn or the individual leaves the school
- Never share biometric data with third parties

A biometric system's log and consent records are maintained by the DPO.

12. Data Protection by Design and Default

We integrate data protection into all school processes by:

- Maintaining a **Record of Processing Activities (ROPA)**
- Conducting **Data Protection Impact Assessments (DPIAs)** for new or high-risk processing
- Ensuring only necessary data is processed for each purpose
- Embedding data protection into all policies and forms
- Providing regular staff training and compliance audits

13. Data Security, CCTV and Storage of Records

Personal data is secured against unauthorised access, alteration, disclosure, or loss.

Measures include:

- Locked storage for paper records
- Password-protected and encrypted digital devices
- Secure sign-out procedures for off-site use
- Regular password updates and access reviews
- Encryption of all portable devices
- Due diligence and secure contracts for third-party processors

CCTV and Surveillance

The Oaks operates CCTV for safety and security, in line with the **ICO's Surveillance Camera Code of Practice**.
Images are stored securely and retained for a limited period before being overwritten.
Access to CCTV footage is strictly controlled and available only to authorised staff or law enforcement.

14. Retention and Disposal of Records

We retain data only for as long as necessary.
Retention periods are guided by the **Information and Records Management Society (IRMS) Toolkit for Schools** and documented by the DPO.

Data no longer required will be securely destroyed by shredding, deletion, or certified third-party disposal.

15. Personal Data Breaches

All suspected or actual breaches must be reported to the DPO immediately.
The DPO will investigate, mitigate the impact, and determine whether to notify the ICO within **72 hours**.
Procedures are detailed in **Appendix 1**.

16. Training

All staff and governors receive data protection training upon induction and refresher training regularly or when legislation or policy changes occur.

17. Monitoring Arrangements

The DPO monitors and reviews this policy and related data protection practices annually.
This policy will be reviewed every **two years**, or sooner if legislation changes, and approved by the governing body.

18. Links with Other Policies

This policy is linked to:

- Online Safety & Acceptable Use Policy
- Staff Code of Conduct
- Safeguarding and Child Protection Policy
- Recruitment and Workforce Privacy Notices
- Parent Privacy Notice

---

19. Appendix 1 – Personal Data Breach Procedure

The Oaks follows the **ICO's guidance on managing personal data breaches**.
Key steps include:

1. Immediate notification to the DPO of any suspected or actual breach.
2. DPO investigates, assesses risk, and logs the incident.
3. If rights and freedoms are at risk, the DPO reports to the ICO within 72 hours.
4. High-risk breaches are communicated to affected individuals promptly.
5. Records of all breaches, regardless of severity, are retained on the admin server.
6. Lessons learned are reviewed to prevent recurrence.