

Tel: 01535 603868
Headteacher: Mrs L Murphy
Email: admin@footprintsfed.com

Tel: 01535 603986
Headteacher: Miss D Ward
Email: office@footprintsfed.com



Data Protection, GDPR & Freedom of Information Policy

1. Purpose and Scope

This policy ensures that our school collects, processes, stores, and deletes personal data in accordance with statutory requirements, including the **UK General Data Protection Regulation (UK GDPR)**, the **Data Protection Act 2018**, and relevant retention laws. This policy applies to all personal data handled by the school regarding pupils, parents, staff, governors, and visitors.

2. Core Data Protection Principles

We process personal data in strict compliance with the six core principles of the GDPR. Data must be:

1. **Lawful, fair, and transparent:** Processed with a valid legal basis and clear communication.
2. **Purpose limitation:** Collected only for specified, explicit, and legitimate school purposes.
3. **Data minimisation:** Adequate, relevant, and limited to only what is necessary.
4. **Accuracy:** Kept accurate and, where necessary, up to date.
5. **Storage limitation (Retention):** Kept in a form that identifies individuals for no longer than is necessary.
6. **Integrity and confidentiality:** Handled securely to prevent unauthorized access, loss, or damage.

3. Data Retention and Disposal

The school maintains a strict Data Retention Schedule in compliance with the *Information and Records Management Society (IRMS) Toolkit for Schools*. Data will not be kept indefinitely.

Record Type	Retention Period	Statutory/Legal Basis
Pupil Child Protection Record	Retained until the pupil reaches the age of 25 .	Education (Pupil Information) Regulations
Special Educational Needs (SEN) Records	Retained until the pupil reaches the age of 25 (or 31 if an EHCP was active).	Limitation Act 1980 / SEND Regulations
School Trip Risk Assessments & Forms	14 years after the date of the trip (if a minor incident occurs) or 25 years if a major incident occurs.	Health and Safety Executive (HSE) & Limitation Act 1980

Record Type	Retention Period	Statutory/Legal Basis
Staff Personnel Files	6 years after termination of employment.	Limitation Act 1980
Governing Body Minutes	Permanently (Archived as historical record).	Statutory Requirement
DBS Certificate Number & Date	Kept on the Single Central Record (SCR) for the duration of employment – move to leavers TAB on leaving and retain for a further 6 months.	Keeping Children Safe in Education (KCSIE)

Secure Disposal: When the retention period expires, files must be securely destroyed. Paper records must be shredded on-site or via a certified confidential waste contractor. Electronic records must be permanently deleted from all active systems, backups, and cloud storage.

4. Staff Records & DBS Information Retention

The school balance its safeguarding duties (*Keeping Children Safe in Education*) with UK GDPR storage limitation principles.

DBS Retention Rules: The physical or digital **DBS Certificate itself** contains highly sensitive criminal record data.

Statutory Rule: The school must **not** keep copies of DBS certificates

What the School **MUST** Retain Separately

The school is legally required to maintain a **Single Central Record (SCR)** of pre-employment checks. The following information must be kept on the SCR for the duration of the staff member's employment and archived according to personnel file timelines:

- The date the DBS check was completed and verified.
- The unique **DBS Certificate Number**.
- The type of check requested (e.g., Enhanced with Barred Lists).
- The name and identity of the individual checked.
- Who conducted the verification check?

5. Bluetooth Trackers (Apple AirTags) & School Trips

5.1 Statement of Policy

The school **strictly prohibits** the use of personal Bluetooth tracking devices—including Apple AirTags, Samsung SmartTags, and Tile trackers—by staff, volunteers, or parents to track children, or groups of children, during school trips, residential visits, or daily school activities.

5.2 Why Unsanctioned Tracking Breaches GDPR

Using these consumer devices to monitor a child or a group of children on a school trip creates severe data protection breaches and safeguarding vulnerabilities:

- **Lack of a Lawful Basis & Consent:** The school is the legally designated Data Controller for pupils during a school trip. Allowing an individual parent or a staff member to track a child via a personal Apple account constitutes unlawful processing of a minor's geolocation data under GDPR Article 6 (Lawfulness) and Article 8 (Children's Consent).
- **Mass Data Breach of Third Parties:** A Bluetooth tracker does not just track one child; it tracks the exact, real-time location of the **entire group of children and staff** traveling with that child. If a parent or unauthorised individual views this data, the privacy of the remaining children and staff is compromised without their knowledge or consent.
- **The "Find My" Network Vulnerability:** AirTags operate by broadcasting unencrypted Bluetooth identifiers to *any* nearby Apple device. This creates an unquantifiable safeguarding risk, potentially allowing unauthorized third parties in the vicinity to detect the presence and movement of a cluster of school children.
- **Proportionality and Security (Article 32):** Consumer tracking devices lack enterprise-grade access controls, audit logs, and data security protocols required for processing vulnerable children's data.

5.3 Operational Rules for Trips

1. **Parents:** Parents are explicitly forbidden from hiding AirTags or trackers in their children's clothing, bags, or belongings for school trips.
2. **Staff Responsibilities:** If a staff member detects or is notified of an unauthorised tracking device travelling with the school group, they are authorised to locate, disable, or remove the battery from the device immediately to protect the privacy of the group.
3. **School-Sanctioned Tracking:** In highly exceptional circumstances where location tracking is required for safety (e.g., specific high-risk wilderness residential trips), the school will only utilise specialised, encrypted, school-owned enterprise equipment. This will be backed by a formal **Data Protection Impact Assessment (DPIA)** and explicit, verifiable parental consent.

6. Subject Access Requests (SARs) and Data Breaches

- **SARs:** Individuals (or parents acting on behalf of primary-aged children) have the right to access their personal data. The school will respond to valid SARs free of charge and within **one calendar month**.
- **Data Breaches:** Any suspected or actual loss of personal data (e.g., misdirected emails, lost physical files, or unauthorised tracking data exposure) must be reported to the school's **Data Protection Officer (DPO)** immediately. If the breach poses a risk to individuals' rights and freedoms, the school will notify the **Information Commissioner's Office (ICO)** within **72 hours**.