Data Protection Impact Assessment (DPIA)

System: Inventory Sign-in System (Staff and Visitor Sign-in)
Organisation: Schools for Every Child Trust
Date: January 2026

1. Purpose

The purpose of this DPIA is to identify and reduce privacy and data protection risks arising from the use of an electronic sign-in system used by staff and visitors across Trust schools. The system is used to manage site safety, safeguarding, access control, and emergency evacuation information.

2. Project overview

The Inventory Sign-in System is a digital platform used at school reception points (and, where applicable, via kiosks or tablets) to record who is on site. It supports:

- Visitor management (sign-in, badges, host notifications where enabled)
- Staff sign-in and site presence tracking (where enabled)
- Safeguarding and access control (knowing who is on site, verifying identity where appropriate)
- Health and safety and emergency evacuation (accurate on-site list)
- Incident management (supporting investigations when required)

3. Data processing description

3.1 Data subjects

- Visitors (parents/carers, contractors, volunteers, supply staff, external professionals)
- Staff (employees, agency staff, peripatetic staff)

3.2 Personal data collected (as stated)

- Name
- Car registration number
- Photograph (for identification and badge printing)
- Email address

3.3 Additional data typically processed (operationally required)

- Time and date of arrival/departure
- Reason for visit and/or person being visited (where enabled)

- Site location (which school/building)
- Visitor category (contractor, volunteer, parent, etc.)
- Badge/ID number (system generated)
- Optional: organisation/company name (contractors)
- Optional: safeguarding declarations (for example, visitor badge type, “DBS seen” indicator), where used

Special category data: Not intended to be collected. The system must not be used to record health information, safeguarding case details, or other special category data in free text fields.

Biometric data: A photo is not treated as biometric data unless it is used for automated facial recognition or unique biometric identification. The Trust will not use facial recognition features (if offered) within this system.

3.4 How the data is used

- To maintain a live, accurate record of who is on site
- To support visitor identification (including badge printing)
- To support site security and safeguarding (controlled access and audit trail)
- To support emergency evacuation and incident response
- To provide records if required for investigations, complaints, safeguarding enquiries, or health and safety matters

3.5 Data storage, location, and access

- Data is stored in the supplier’s hosted environment (cloud) or Trust-hosted environment (depending on the supplier model).
- Access is restricted to authorised staff only (typically reception staff, school leaders, site team, and central Trust staff where required).
- The system must use secure logins and role-based permissions.
- Administrative access must be limited to named roles and reviewed regularly.

4. Lawful basis and fairness

4.1 Lawful basis (UK GDPR Article 6)

Visitors and contractors

- **Article 6(1)(c) Legal obligation:** Health and safety duties, safeguarding expectations, and managing site safety.
- **Article 6(1)(f) Legitimate interests:** Ensuring site security, maintaining an audit trail, and protecting pupils, staff, and visitors.

Staff (where staff sign-in is used)

- **Article 6(1)(c) Legal obligation:** Health and safety and duty of care.

- **Article 6(1)(b) Contract:** Where sign-in supports operational and contractual expectations (for example, workforce deployment and site management).
- **Article 6(1)(f) Legitimate interests:** Safety, security, and emergency planning.

4.2 Transparency

- Signage at reception and a short privacy notice must explain what is collected, why, retention, and who to contact.
- A fuller privacy notice should be available via school websites or on request.

5. Necessity and proportionality

The data items collected are proportionate to the purpose:

- **Name** is necessary to identify the individual on site.
- **Car registration** supports site safety and security (for example, parking issues, emergency situations, or incident response).
- **Photo** supports accurate identification and badge control, reducing the risk of unauthorised access.
- **Email** supports operational contact (for example, pre-registration, confirmations, and follow-up if needed).

Controls will be put in place to avoid collecting data that is not required and to prevent free-text fields being used to store inappropriate information.

6. Risk assessment and mitigation

Risk area	Risk description	Mitigation / control
Unauthorised access	Staff without a need to know access visitor logs or personal data	Role-based access, least-privilege permissions, named admin roles, regular access reviews, strong passwords and MFA where available
Data breach	Loss or exposure of visitor log data (names, emails, photos, car regs)	Supplier security assurances, encryption in transit and at rest, audit logs, incident response process, staff training, device security for kiosks/tablets
Over-collection	Capturing unnecessary details (especially in free text)	Disable unnecessary fields, limit free-text, staff guidance, periodic checks by school DPO lead
Inaccurate records	Incorrect sign-in details causes safeguarding or emergency risks	Reception oversight, visitor verification steps, clear prompts, option to correct entries, routine checks

Retention creep	Data stored longer than needed	Set retention rules in system, routine deletion schedule, documented retention period, annual review
Visitor privacy	Visitors unaware of photo capture or email usage	Clear signage and privacy notice at point of collection; staff explanation if asked
Supplier/processor risk	Supplier not meeting UK GDPR standards or unclear data location	Data Processing Agreement (DPA), due diligence (security, hosting, sub-processors), ensure UK GDPR compliant terms, documented controller-processor roles
Device/kiosk exposure	Someone views prior sign-in details at the kiosk	Kiosk privacy mode, auto-timeout, prevent back navigation, screen positioning, supervised reception
Misuse of photos	Photo used beyond identification (or exported unnecessarily)	Restrict export functions, disable facial recognition, limit photo visibility to authorised roles, policy on use and sharing
Subject rights handling	Difficulty responding to SAR/erasure requests	Clear process with DPO oversight, supplier supports export/search, defined responsibilities and timelines

7. Data retention

Retention must match purpose and Trust records management practice. Suggested baseline:

- **Visitor sign-in records (including email and photo):** 12 months
- **Car registration data:** 3 to 12 months (align to visitor log retention unless a shorter period is justified operationally)
- **Staff sign-in records (if used):** 12 months, unless needed longer for a specific incident or health and safety investigation
- **Incident-linked records:** retained in line with the relevant incident/safeguarding/health and safety record retention requirements

The final retention settings must be confirmed in the system configuration and documented.

8. Security measures (minimum expected)

- Unique user accounts (no shared logins)
- MFA for admin accounts where available

- Role-based access control
- Audit logs enabled
- Encryption in transit (TLS) and at rest
- Secure kiosk configuration: auto-logout, no access to historic records, restricted OS access
- Supplier breach notification procedures and clear escalation route to the Trust
- Regular review of user access and leavers process

9. Roles and responsibilities

- **Data Controller:** Schools for Every Child Trust
- **Data Processor:** The Inventory Sign-in System supplier
- **Local operational owners:** Head of School / Headteacher and Reception Lead at each school
- **Oversight:** Trust Data Protection Officer (or appointed data protection lead)

The Trust remains responsible for ensuring processing is lawful, transparent, and proportionate, and for ensuring contracts and due diligence are in place.

10. DPIA outcome

Overall risk rating (pre-mitigation): Medium
Overall risk rating (post-mitigation): Low to Medium (dependent on supplier assurance, retention controls, and kiosk configuration)

-