Data Protection Impact Assessment (DPIA)

System: Key and Governor Hub (CPD Recording Platform)
Organisation: Schools for Every Child Trust

1. Purpose

The purpose of this DPIA is to identify and mitigate any data protection and privacy risks arising from the use of the **Key and Governor Hub**, a system used to record and manage Continuing Professional Development (CPD) for staff and governors across the Trust.

2. Project overview

The Key and Governor Hub is a digital platform used to:

- Record CPD activity for staff and governors
- Track statutory and non-statutory training completion
- Support governance oversight and assurance
- Evidence compliance with regulatory and safeguarding expectations
- Support workforce development and quality assurance

The system supports Trust-wide visibility of training without storing unnecessary personal or sensitive information.

3. Data processing description

3.1 Data subjects

- Trust staff (including teachers, support staff, leaders, and central team staff)
- Governors and trustees

3.2 Personal data collected

- Name
- Email address
- Role (for example, staff, governor, trustee)
- CPD records (training title, date, completion status, provider)

3.3 Personal data not collected

- Special category data (for example health, ethnicity, political views)
- Safeguarding case information

- Performance management or appraisal commentary

The system is not designed to hold sensitive or special category data, and free-text fields (where present) must not be used to record such information.

3.4 How the data is used

- To maintain an accurate record of CPD undertaken
- To monitor compliance with statutory and Trust-required training
- To support governance assurance and inspection readiness
- To identify training gaps and plan future CPD

4. Lawful basis for processing

4.1 UK GDPR Article 6 lawful bases

Staff

- **Article 6(1)(b) Contract:** CPD and training records form part of employment and professional expectations
- **Article 6(1)(c) Legal obligation:** Certain training is required by law or statutory guidance (for example safeguarding)
- **Article 6(1)(f) Legitimate interests:** Workforce development, quality assurance, and organisational effectiveness

Governors and trustees

- **Article 6(1)(c) Legal obligation:** Governance, safeguarding, and statutory compliance expectations
- **Article 6(1)(f) Legitimate interests:** Effective governance, accountability, and assurance

4.2 Transparency

- Staff and governors are informed through Trust privacy notices that CPD records are held centrally.
- Privacy information is available via Trust and school websites or on request.

5. Necessity and proportionality

The data collected is minimal and proportionate:

- **Names and emails** are required to identify individuals and link CPD records accurately.
- **CPD records** are necessary to evidence training completion and compliance.

No excessive or intrusive data is collected, and the system is not used for monitoring beyond professional development purposes.

6. Risk assessment and mitigation

Risk	Description	Mitigation
Unauthorised access	CPD records accessed by those without a legitimate role	Role-based access controls, restricted admin permissions, regular access reviews
Data breach	Exposure of names, emails, or CPD records	Secure hosting, encryption in transit and at rest, strong passwords, incident response procedures
Over-retention	CPD data retained longer than necessary	Defined retention periods aligned to Trust policy, routine reviews
Inappropriate data entry	Sensitive information entered into CPD notes	Staff guidance, limited free-text fields, periodic checks
Inaccurate records	Incorrect CPD completion status	User access to update records, admin oversight, regular data quality checks
SAR handling	Difficulty responding to subject access requests	Clear internal process, system search/export functionality

7. Data retention

Recommended retention periods (subject to Trust policy):

- **Staff CPD records:** Duration of employment plus 6 years
- **Governor/trustee CPD records:** Term of office plus 6 years

Data will be securely deleted or anonymised once retention periods expire, unless required for legal or regulatory reasons.

8. Security measures

- Secure user authentication
- Role-based permissions
- Restricted administrator access
- Audit logs (where available)
- Supplier security assurances and contractual controls
- Regular review of active users (including leavers)

9. Roles and responsibilities

- **Data Controller:** Schools for Every Child Trust
- **Data Processor:** Key and Governor Hub system provider
- **Operational leads:** Trust governance lead / CPD lead
- **Oversight:** Trust Data Protection Officer (or appointed data protection lead)

The Trust retains overall responsibility for compliance with UK GDPR and the Data Protection Act 2018.

10. DPIA outcome and approval

Overall risk rating (pre-mitigation): Low to Medium
Overall risk rating (post-mitigation): Low