Data Protection Impact Assessment (DPIA) for Smoothwall Safeguarding System

1. Introduction

This DPIA assesses the data protection risks associated with the use of the Smoothwall safeguarding system at Schools for Every Childfor logging concerns.

2. Project Description

Project Name: Smoothwall Safeguarding System
Purpose: To log and manage safeguarding concerns efficiently and securely.
Stakeholders:

- Safeguarding Leads
- IT Department
- Teaching and Support Staff

3. Data Processing

Nature of Data: Personal data concerning students, including names, dates of birth, contact details, and safeguarding concerns.

Context: Data is collected to ensure the safety and well-being of students.
Purpose: To monitor, record, and address safeguarding issues promptly.

4. Data Fl

Data Collection: Staff members log concerns via the Smoothwall system.
Data Storage: Data is stored securely within the Smoothwall system, with access restricted to authorized personnel.
Data Sharing: Information may be shared with relevant authorities, such as social services, when necessary.

5. Consultation Process

Stakeholders Consulted:

- Data Protection Officer (DPO)

6. Necessity and Proportionality

Necessity:

- To fulfil legal obligations under safeguarding legislation.
- To ensure the safety and well-being of students.

Proportionality:

- Data collected is limited to what is necessary for safeguarding purposes.
- Access to data is restricted to authorized personnel only.

7. Identify and Assess Risks

Risk	Likelihood	Impact	Mitigation
Unauthorized access to data	Medium	High	Use of strong passwords, restricted access, regular audits
Data breaches	Low	High	Encryption, regular security updates, staff training
Inaccurate data	Medium	Medium	Regular reviews and updates, staff training

8. Mitigation Measures

- **Access Control:** Implement role-based access controls to ensure only authorized personnel can access sensitive data.
- **Encryption:** Use encryption to protect data both in transit and at rest.
- **Training:** Provide regular training to staff on data protection and safeguarding procedures.
- **Audit:** Conduct regular audits to ensure compliance with data protection policies.
- **Incident Response:** Develop a clear incident response plan to address data breaches promptly.