# Data Protection Impact Assessment (DPIA) Every

## 1. Introduction

**Project Name:** Implementation of Every Risk Register Management System, Health and Safety Software, and Staff CPD Register

## 2. Purpose and Scope

This DPIA assesses the data protection risks associated with the implementation of Every's risk register management system, health and safety software, and staff CPD register. It aims to ensure compliance with the General Data Protection Regulation (GDPR) and to protect the personal data of pupils, staff, and stakeholders.

## 3. Description of Processing

**System/Software Involved:**

- Every Risk Register Management System
- Every Health and Safety Software
- Every Staff CPD Register

**Types of Personal Data Processed:**

- Staff details (names, job titles, qualifications, training records)
- Health and safety incident reports
- Risk assessments
- CPD records

**Purpose of Processing:**

- To manage and record risks effectively
- To ensure compliance with health and safety regulations
- To track and manage staff CPD

## 4. Data Flow and Storage

**Data Collection:**

- Data will be collected from staff members and incident reports.

**Data Storage:**

- Data will be stored securely on Every's cloud-based platform.

**Data Access:**

- Access will be restricted to authorized personnel only.

**Data Retention:**

- Data will be retained in accordance with the school's data retention policy.

**5. Consultation Process**

**Stakeholders Consulted:**

- Staff members
- DPO

**6. Necessity and Proportionality**

**Legal Basis for Processing:**

- Legitimate interests
- Compliance with legal obligations

**Measures to Ensure Data Minimization:**

- Only necessary data will be collected and processed.

**7. Risk Assessment**

| Risk | Likelihood | Impact | Mitigation Measures |
|---|---|---|---|
| Unauthorized access to data | Medium | High | Implement strong access controls and regular audits |
| Data breach | Low | High | Use encryption and secure data storage |
| Data loss | Low | Medium | Regular backups and disaster recovery planning |
| Inaccurate data | Medium | Medium | Regular data validation and staff training |

**8. Data Protection Measures**

- **Access Controls:** Implement role-based access controls to restrict data access to authorized personnel only.
- **Encryption:** Use encryption for data at rest and in transit.

- **Training:** Provide regular data protection training for staff.
- **Audits:** Conduct regular audits to ensure compliance with data protection policies.

**9. Action Plan**

| Action | Responsible Person | Deadline |
|---|---|---|
| Implement access controls | IT Department | [Insert Date] |
| Conduct staff training | HR Department | [Insert Date] |
| Perform data protection audit | DPO | [Insert Date] |