Data Protection Impact Assessment (DPIA) – CPOMS

DPIA in relation to

Use of CPOMS (Child Protection Online Management System) to record, monitor and manage safeguarding and welfare concerns for pupils in school.

Responsible individuals

Headteacher: Laura Concannon – Overall accountability

Designated Safeguarding Lead (DSL): Laura Concannon – System lead

Data Protection Officer: Louise King – Compliance oversight

IT Technician – Stone

Assessment date

07 June 2026

Review date

Annually or when changes to safeguarding processes occur

Step 1: Need for DPIA

CPOMS processes highly sensitive safeguarding and special category data relating to children, including safeguarding concerns, SEN and health data. This constitutes high-risk processing involving vulnerable individuals (children). A DPIA is required due to the large-scale processing of sensitive data. Benefits include improved safeguarding, centralised records, early identification of risks and secure information sharing.

Step 2: Processing

Collection: Data entered by school staff when concerns arise, and imported from MIS systems.

Usage: Recording safeguarding concerns, tracking incidents, building chronologies, supporting DSL decision-making.

Storage: Secure cloud-based system with role-based access and encryption.

Deletion: In line with retention schedule and safeguarding policy.
Sharing: With safeguarding partners such as Local Authority, social care, and external agencies where required.
High Risk: Processing of special category safeguarding data for children.

Scope

Data includes personal and special category data such as names, DOB, safeguarding concerns, health information, SEN and behavioural incidents. Data relates to all pupils and limited staff/parent information. Data is collected continuously as incidents arise and retained in line with safeguarding retention requirements. Data is stored securely within UK/EU compliant systems.

Context

Processing involves children, a vulnerable group, in a duty-of-care relationship. Staff are legally required to record safeguarding concerns and would expect the use of such systems. CPOMS is widely used and not novel technology. There is strong public expectation that safeguarding data is handled securely.

Purpose

To ensure effective safeguarding of pupils by recording, monitoring and acting on concerns. Benefits include improved child protection, faster response times, better communication and reduced administrative burden.

Step 3: Consultation

Consultation with Senior Leadership Team, Designated Safeguarding Lead, IT provider and Data Protection Officer. Parents informed through privacy notices. Direct consultation not required as processing is necessary for safeguarding and legal obligations.

Step 4: Necessity and proportionality

Lawful basis: Public task and legal obligation. Special category condition: substantial public interest (safeguarding). Data minimisation ensured through staff training and policy. Access restricted via permissions and audited regularly. Privacy notices inform individuals. Rights supported through school GDPR procedures. Data processor agreement in place with CPOMS.

Step 5: Risks

Unauthorised access to safeguarding records (high), data breach (medium), misuse of sensitive information (medium), inaccurate recording (low). Risks include harm to individuals, loss of confidentiality and reputational damage.

Step 6: Mitigations

Role-based access controls, two-factor authentication, staff safeguarding and GDPR training, secure cloud hosting, audit logs and monitoring, strict data sharing protocols. Residual risk reduced to low.

Step 7: Sign off

Headteacher: Laura Concannon Date: 7/06/2026