SUTTON VALENCE SCHOOL
SINCE 1576

Data Protection Impact Assessment Policy and Procedure

(Prep School and Senior School)

Author: Mr Glen Millbery
Policy review date: September 2025
Approval date by Governors: November 2025
Next Review Date: September 2026

This Policy applies to Sutton Valence School (including as the context requires, the Nursery, the Prep School and Senior School).

1 Purpose

This policy and procedure establishes an effective, accountable and transparent framework for ensuring compliance with the requirements for data protection impact assessment by the GDPR.

2 Policy Statement

Data Protection Impact Assessments (DPIAs) are used to identify and mitigate against any data protection related risks arising from a new project, service, product, or process which may affect the organisation (data controller) or the individuals (data subjects).

When is a DPIA necessary

2.1 A DPIA is necessary:

- Before the implementation of new technologies or processes, or before the modification of existing technologies or processes where the data processing is likely to result in a high risk to the rights and freedoms of individuals.

2.2 Processing that is likely to result in a high risk includes (but is not limited to):

- Systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals;
- Large scale processing of special categories of data or personal data in relation to criminal convictions or offences;
- Large scale, systematic monitoring of public areas (CCTV).

2.3 A record of the DPIA and must be kept and available for audit or investigation.

3 Procedure

It is anticipated that a DPIA will not be completed in isolation but will be completed by the individual requiring the use of the personal data and the Data Compliance Officer.

Steps for conducting a DPIA

3.1 **Describe data usage.** Identify how personal information will be collected, stored, used and deleted as part of the new (or modified) system or process. Identify what kinds of data will be used as part of the new (or modified) system or process and who will have access to the data.

3.2 **Identify data protection and related risks.** Identify all risks to data subjects or to the organisation (data controller) that are related to personal data protection.

3.3 **Assign risk mitigation measures – privacy solutions.** For each risk assign solutions to reduce or eliminate the risk.

3.4 **Follow up actions:** If the risk is accepted then detail the next steps and record approval.

3.5 **Approval:** The DPIA is agreed by all parties that use the data and signed by them. It is signed by the DCO and final approval and impartial check conducted by the Bursar.

3.6 **Further actions:** DPIAs should be included as part of the annual reporting process to Governors.

Completed DPIAs are stored in GDPR Sentry.