Data Protection Policy

Version History	
Date of first issue:	March 2018
Dates of Updates:	February 2019, September 2021, February 2024, February 2026
Most recently approved by governors on:	March 2026
To be next reviewed on:	March 2027

Contents

Data Protection Policy

1 Legal Obligations

Recital 74 of the UK General Data Protection Regulation (UK GDPR) states that……

> *'The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with the Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons'*

To this end, the School and the School Governing Body has adopted the Policy as specified below.

2 Data (Use and Access) Act 2025 (DUAA 2025)

The Data (Use and Access) Act 2025 (DUAA) complements the UK Data Protection Act 2018 (DPA) and UK GDPR by refining and modernizing the existing framework rather than replacing it. It received Royal Assent on 19 June 2025.

The changes include clarifications on using personal data for research, lifting restrictions on automated decision-making with appropriate safeguards, and allowing some cookies without consent. The Information Commissioner's Office (ICO) is also restructured as a body corporate called the Information Commission.

3 Requirements for Schools under the Data (Use and Access) Act 2025

Focussing on the DUAA 2025 and implications for the school this policy highlights the following:

Handling Complaints: The DUAA 2025 mandates that individuals must first complain directly to the school before contacting the ICO regarding data rights. Clause 103 of DUAA inserts a new section 164A into the UK DPA 2018, to introduce requirements for how schools must facilitate and handle complaints under the UK GDPR or DPA 2018, Pt 3. It will be a requirement of Sutton School to provide an electronic complaints form for individuals who wish to raise concerns about how their personal data is handled.

According to the Information Commission (1) The school must provide a way for individuals to submit complaints electronically (e.g. via a web form) and (2) The school must acknowledge complaints within 30 days. The school must respond "without undue delay."

Recognised Legitimate Interests: A Legitimate Interest Assessment (LIA) is one of six lawful basis under Article 6 of the UK GDPR where no other appropriate lawful basis can be used by the School in the following circumstances, e.g. use of ParentMail to communicate with parents, use of Tucasi and processing of school meal payments, etc. Undertaking an LIA involves the purpose test, the necessity test and the balancing test.

Previously a Legitimate Interest Assessment would be used in the circumstances outlined above. Under the Recognised Legitimate Interests, it is now acknowledged that this is no longer necessary. However, there may be specific circumstances where there may be a need to complete a bespoke Legitimate Interests Assessment where a Recognised Legitimate Interest may fit not the particular situation or requirement. These would be dealt with on a case-by-case basis.

Subject Access Requests: The DUAA 2025 has updated Article 15 of the UK GDPR (Article 15(1A)) to make it clear that data subjects are only entitled to such confirmation, personal data and other information as the controller is able to provide based on a reasonable and proportionate search for the personal data. Sutton School will determine whether the required search is neither reasonable nor proportionate.

4 Scope

An essential activity within **Sutton School** is the requirement to gather and process information about its pupils, staff, parents and other individuals who have contact with the school, in order to enable it to provide education and other associated functions.

In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

The UK GDPR defines special category information as *'information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data'*.

Before processing 'special category' information **Sutton School** will identify and document the lawful basis for processing this information. **Sutton School** will only process special categories of personal information in certain situations.

This will be done in accordance with Data Protection Law and other related government legislation.

This policy applies to employees and pupils of **Sutton School**. It also applies to visitors, temporary staff, volunteers and Governors working on behalf of the school.

Sutton School and the School Governing Body – acting as custodians of personal data – recognise their moral duty to ensure that it is handled properly and confidentially at all times, irrespective of whether it is held on paper or by electronic means. This covers the whole lifecycle, including:

- The obtaining of personal data;
- The storage and security of personal data;
- The use of personal data;
- The disposal/destruction of personal data.

Sutton School and the School Governing Body also has a responsibility to ensure that data subjects have appropriate access to details regarding personal information relating to them.

5 Objectives

By following and maintaining strict safeguards and controls, **Sutton School** and the School Governing Body will:

- Acknowledge the rights of individuals to whom personal data relate, and ensure that these rights may be exercised in accordance with Data Protection Law;
- Ensure that individuals are fully informed about the collection and use of personal data through the publication of the school's Privacy Notice;
- Collect and process personal data which is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Ensure that adequate steps are taken to ensure the accuracy and currency of data;
- Ensure that for all personal data, appropriate security measures are taken – both technically and organisationally – to protect against damage, loss or abuse;
- Ensure that the movement of personal data is done in a lawful way – both inside and outside the organisation and that suitable safeguards exist at all times.

6 Achieved by

In order to support these objectives, Sutton School and the School Governing Body will:

- Have a **"Senior Information Risk Owner"** (SIRO) to ensure that there is accountability and that Information Risk is recognised at a Senior Level;
- Have a designated **"Data Protection Officer**" (DPO) to meet the school's obligations under Article 37 of UK GDPR
- Ensure that all activities that relate to the processing of personal data have appropriate safeguards and controls in place to ensure information security and compliance with the Data Protection Law;
- Ensure that all contracts and service level agreements between Sutton School and external third parties (including contract staff – where personal data is processed) include the relevant Data Protection clauses and appropriate Organisational and Technological measures will be put in place to safeguard the data*;*
- Ensure that all staff (**including volunteer staff**) acting on behalf of Sutton School understand their responsibilities regarding information security under the Act, and that they receive the appropriate training/instruction and supervision so that they carry these duties out effectively and consistently and are given access to personal information that is appropriate to the duties they undertake;
- Ensure that all third parties acting on Sutton Schools behalf are given access to personal information that is appropriate to the duties they undertake and no more;
- Ensure that any requests for access to personal data are handled courteously, promptly and appropriately, ensuring that either the data subject or their authorised representative have a legitimate right to access under Data Protection Law, that their request is valid, and that information provided is clear and unambiguous;
- Ensure that all staff are aware of the Data Protection Policy and Guidance;.
- Review this policy and the safeguards and controls that relate to it annually to ensure that they are still relevant, efficient and effective.
- This Policy and Procedure and the Subject Access Information material will be made available in other formats where necessary.

Please follow this link to the ICO's website which provides further detailed guidance on a range of topics including individual's rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc.

7 AI and Data Protection

To manage the risks to rights and freedom of individuals that arise from processing personal data in a school's AI system, it is important that the school understand the fundamental rights, risks, and how to balance these and other interests. Ultimately, it is necessary for the school to:

- assess the risks to individual rights that the use of AI poses;
- determine how the school will address these; and
- establish the impact this has on the school's use of AI.
- The school should ensure its approach fits both the school as data controller and the circumstances of the data processing. Where appropriate, the school should also use risk assessment frameworks.

For further information please see Appendix 1: Artificial Intelligence (AI) – Data Protection Considerations

8 Supporting Guidance Documents

The following guidance documents are directly relevant to this policy.

- E-Safety Policy for Schools
- Generative Artificial Intelligence Guidance
- Guidance for use of Passwords in School
- Homeworking Guidance
- Protective Marking
- Information Asset Registers
- Security Incident Reporting Guidance
- Policy Governing the operation of CCTV

9 Version Control

This policy will be evaluated on a regular basis.

This version of the policy is based on YourIG Data Protection Policy v6.0.

10 Further Information

We may change this policy from time to time.

If you have any questions or concerns about how we use your personal information, please contact:

- YourIG Data Protection Officer Service,
- Dudley MBC,
  The Council House,
  Dudley,
  DY1 1HF
- Email: YourIGDPOService@dudley.gov.uk
- Tel: 01384 815026

You also have the right to complain to the Information Commissioner's Office if you're unhappy about how we process your information.

11 Appendix 1: Artificial Intelligence (AI) – Data Protection Considerations

As Artificial Intelligence (AI) tools become more common in education, the school recognises its duty to ensure their use is fully compliant with the UK General Data Protection Regulation (UK GDPR) and aligned with its safeguarding responsibilities.

This appendix outlines how the school manage AI use with regard to the processing of personal data.

11.1 Purpose and Scope

This guidance applies to all staff, governors, and third-party providers who may interact with AI tools or systems as part of school activities. It covers any AI technologies, including:

- Generative AI (e.g. tools that create text, images, or video).
- Predictive tools (e.g. analytics software).
- Automated marking or feedback systems.
- Any AI features embedded within digital platforms used by the school.

11.2 Key Safeguards for Pupil Data

To protect pupils and their data, the following rules apply:

a. Age Restrictions

- Pupils will not have access to any generative AI tool or platform that has an age restriction above their current age, including 13+, 16+, or 18+ rated tools.
- Staff must verify the suitability and age-appropriateness of any tool used in the classroom.

b. No Personal Data Shared with AI Models

- No personal data about pupils will be entered into or shared with any AI model, regardless of whether it is hosted on a school device, cloud-based, or externally provided.
- This includes:
    - Full names
    - Contact information
    - Photographs or videos
    - Identifiable written work or behaviour data
    - Health, SEND or safeguarding information

If AI is used in any school system, it must be fully assessed for data protection compliance and explicitly configured to exclude identifiable pupil information.

11.3 Legal Basis and GDPR Principles

Any AI use involving school-held data must comply with the seven principles of the UK GDPR, including:

- Lawfulness, fairness and transparency: The school must inform individuals if AI is used to process their data.
- Purpose limitation & data minimisation: AI tools must only use the minimum data required for clearly defined educational purposes.
- Accuracy & accountability: All outputs must be reviewed by staff; AI must not be used to make unsupervised decisions.
- Integrity and confidentiality: AI services must meet the school's security and data hosting standards (e.g. UK/EU servers).

11.4 Staff Responsibilities

Staff must:

- Only use AI tools approved by the school leadership and DPO.
- Avoid entering any personal, confidential or sensitive information into AI systems.
- Review and verify any AI-generated content before sharing or using it in the classroom.
- Seek advice from the Data Protection Officer (DPO) before using new AI tools, especially those involving pupil interaction or data.

11.5 Third-Party AI Tools and Providers

Before adopting or trialling any AI-enabled service, the school will:

- Conduct a Data Protection Impact Assessment (DPIA) where personal data may be processed.
- Ensure data processing agreements are in place.
- Confirm that data will not be used to train or improve external AI models unless fully anonymised and legally compliant.

11.6 Automated Decision-Making

The school does not use AI to make decisions about individuals without human involvement.

Where AI is used to inform teaching or administrative actions, final decisions will always be made by staff.

11.7 Ongoing Oversight and Review

- AI use will be monitored by the DPO and Online Safety Lead to ensure compliance and identify new risks.
- This appendix will be reviewed annually or as AI usage in education evolves.

Support and Resources

- ICO AI Guidance
- Data Protection in Schools
- YourIG Generative Artificial Intelligence (AI)