STOUR VALE ACADEMY TRUST

DATA PROTECTION POLICY

VERSION / DATE	VERSION 2.4 SEPTEMBER 2026
NEXT VERSION DUE BY	MARCH 2029

Contents

Legal Obligations 3
Data (Use and Access) Act 2025 (DUAA) 3
Requirements for schools under the Data (Use and Access) Act 2025 3
Scope 4
Objectives 5
Achieved by 5
AI and Data Protection 6
Supporting guidance documents 6
Version Control 7
Further information 7

Data Protection Policy for Stour Vale Academy Trust

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, Stour Vale Academy Trust ('the Trust'), comprising the member schools, settings and the central team, has adopted the Policy as specified below.

Data (Use and Access) Act 2025 (DUAA)

The Data (Use and Access) Act 2025 (DUAA) complements the UK Data Protection Act 2018 (DPA) and UK GDPR by refining and modernising 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.

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

This policy highlights the following with reference to the DUAA 2025:

Handling complaints: The DUAA 2025 mandates that individuals must first complain directly to the Trust 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. The Trust is required to provide an electronic complaints form for individuals who wish to raise concerns about how their personal data is handled. A link to that form is available in Appendix 1 of the Stour Vale Complaints Policy (section entitled 'Complaints about processing of personal data').

According to the Information Commission:

1. schools must provide a way for individuals to submit complaints electronically (i.e. via a web-based form); and
2. schools must acknowledge complaints within 30 days and respond 'without undue delay'.

Recognised Legitimate Interests: A Legitimate Interest Assessment (LIA) is one of six lawful bases under Article 6 of the UK GDPR and is used where there is no other appropriate lawful basis, e.g. use of parental communication apps to send messages to

parents or use of payment apps to process school meal payments. An LIA involves undertaking 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 in which a bespoke Legitimate Interests Assessment must be completed, where the Recognised Legitimate Interest does not fit 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.* We will determine whether the required search is neither reasonable nor proportionate.

Scope

An essential activity within the Trust is the requirement to gather and process information about its pupils, staff, parents and other individuals who have contact with it, 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 Trust 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 the Trust will identify and document the lawful basis for processing this information. The Trust will process special categories of personal information only 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 the Trust. It also applies to temporary staff, volunteers, and members, trustees and governors working on behalf of the Trust.

The Trust – acting as a custodian of personal data – recognises its 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.

The Trust also has a responsibility to ensure that data subjects have appropriate access to details regarding personal information relating to them.

Objectives

By following and maintaining strict safeguards and controls, the Trust 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 Trust's Privacy Notices;
- 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.

Achieved by

In order to support these objectives, the Trust will:

- have **'Senior Information Risk Owners'** (SIROs) 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 Trust'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 Data Protection Law;
- ensure that all contracts and service level agreements between the Trust 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 the Trust 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 the Trust's 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 every three years or more frequently as required, 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 individuals' rights, exemptions from the Act, dealing with subject access requests, and how to handle requests from third parties for personal data to be disclosed.

AI and Data Protection

To manage the risks to rights and freedom of individuals that arise from processing personal data in AI systems used within the Trust, it is important for the Trust to understand the fundamental rights and risks, and how to balance these and other interests. Ultimately the Trust must:

- assess the risks to individual rights that the use of AI presents;
- determine how it will address these; and
- establish the impact this has on its use of AI.

The Trust should ensure its approach fits both its duties as data controller and the circumstances of the data processing. Where appropriate, the Trust should also use risk assessment frameworks.

Staff will adhere to the requirements set out in the Stour Vale Principles for Use of Generative AI.

Supporting guidance documents

- Stour Vale Dealing with a Security Incident Guidance
- Stour Vale Principles for Use of Generative AI

- Stour Vale Subject Access Request Policy
- Information Asset Registers

Version Control

This policy will be reviewed and approved every three years or more frequently as required.

Further information

For further information, please contact:

YourIG Data Protection Officer Service
Dudley MBC, The Council House, Dudley, West Midlands, DY1 1HF
Email: YourIGDPOService@dudley.gov.uk Tel: 01384 815607