Data Protection Appropriate Policy Document (APD)

Date ratified	April 2026
Committee Responsible for Policy	Business Committee and FGB
Date to be updated	April 2027
Headteacher Signature	
Chair of Governors/ Committee Signature	

Holy Trinity has adopted the Merton model APD November 2022

1 Introduction

1.1 Schedule 1, Part 4 of the Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category data and criminal offence data under certain specified conditions. This is the 'Appropriate Policy Document' for Holy Trinity C of E Primary School

1.2 The purpose of this statutory policy is to explain the basis on which we process special category and criminal convictions data and to demonstrate that our processing is compliant with principles set out in data protection legislation.

1.3 This policy has been updated to reflect amendments introduced by the Data (Use and Access) Act 2025 (DUAA), which received Royal Assent on 19 June 2025. The DUAA amends the UK GDPR and DPA 2018 but does not replace them

2 Special category data

2.1 Special category data is defined as personal data revealing:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (where used for identification purposes)
- Data concerning health, or
- Data concerning a natural person's sex life or sexual orientation.

3 Criminal convictions and offences data

3.1 Article 10 GDPR covers processing in relation to criminal convictions and offences. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes "*personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing*". This is collectively referred to as 'criminal offence data'.

4 Conditions for processing special category and criminal offence data

4.1 Within the UK GDPR, all processing of special category data must meet an Article 9(2) condition in order for that processing to be lawful. The Article 9(2) conditions for processing special category data are:

- Article 9(2)(a) Explicit consent
- Article 9(2)(b) Employment, social security and social protection
- Article 9(2)(c) Vital interests

- Article 9(2)(d) Not-for-profit bodies
- Article 9(2)(e) Made public by the data subject
- Article 9(2)(f) Legal claims or judicial acts
- Article 9(2)(g) Reasons of substantial public interest (with a basis in law)
- Article 9(2)(h) Health or social care (with a basis in law)
- Article 9(2)(i) Public health (with a basis in law)
- Article 9(2)(j) Archiving, research and statistics (with a basis in law)

4.2 If processing is reliant on conditions (b), (h), (i) or (j), an associated condition in UK law, set out in Part 1 of Schedule 1 of the DPA 2018 must be met.

4.3 If processing is reliant on Article 9(2)(g) Reasons of substantial public interest, an associated condition in UK law, set out in Part 2 of Schedule 1 of the DPA 2018 must be met.

4.4 The school processes special category data under the following Article 9 and Schedule 1 conditions:

Article 9 condition	**Examples of Processing**	**Schedule 1 Condition (where required)**
Article 9(2)(a) data subject has given explicit consent	E.g. processing pupil and staff dietary requirements or consent for pupil pastoral support.	Not required
Article 9(2)(b) necessary in the field of employment law.	E.g. processing staff sickness absences, recording details of trade union membership, processing criminal offence data for the purposes of preemployment checks and declarations by an employee in line with contractual obligations.	**Part 1, Schedule 1 condition:** Para 1: Employment, social security and social protection
Article 9(2)(c) necessary to protect the vital interests of the data subject	E.g. using health information about a member of staff or a student in a medical emergency.	Not required
Article 9(2)(f) necessary for the establishment, exercise or defence of legal claims.	E.g. processing relating to any employment tribunal or other litigation.	Not required

Article 9(2)(g) necessary for reasons of substantial public interest.	E.g. processing student health information in order to ensure they receive appropriate educational support. Identifying individuals at risk by recording and reporting concerns from pupils and staff Obtaining further support for children and individuals at risk by sharing information with relevant agencies.	**Part 2, Schedule 1 conditions:** Para 6(1) and (2)(a): Statutory etc. and government purposes Para 8(1) and (2): Equality of opportunity or treatment Para 10(1): Preventing or detecting unlawful acts Para 16(1): Support for individuals with a particular disability or medical condition Para 18(1): Safeguarding of children and of individuals at risk
Article 9(2)(h)	E.g. the provision of occupational health services to our employees.	**Part 1, Schedule 1 condition:**
Article 9 condition	**Examples of Processing**	**Schedule 1 Condition (where required)**
necessary to assess the working capacity of the employee.		Para 1: Employment, social security and social protection
Article 9(2)(j) for archiving purposes in the public interest.	E.g. maintaining a school archive of photos and significant school events for historical purposes.	**Part 1, Schedule 1 condition:** Paragraph 4 Research etc

5 How we are compliant with the data protection principles

5.1 Principle (a): Lawfulness, fairness and transparency.

The school will ensure that:

- for each occasion where we process personal data, we have established the lawful basis of the processing under the UK GDPR
- where our processing is based on explicit consent, we have taken steps to ensure clear, freely given consent has been given and is recorded. We have made it clear to all parties how consent can easily be withdrawn at any time
- we provide clear and transparent information about why we process personal data through our privacy notices and associated policies
- a Data Protection Policy is established for the protection of personal data held within Holy Trinity C of E Primary School. This has been approved by governors and communicated to all employees and other relevant people.

5.2 Principle (b): Purpose limitation

The school will ensure that:

- we only collect personal data for specified, explicit and legitimate purposes, and, having regard for the purpose of the processing, we will inform data subjects what those purposes are in a privacy notice
- we do not use personal data for purposes that are incompatible with the purposes for which it was collected. If we do use personal data for a new purpose that is compatible, and having regard for the purpose of the processing, we will inform the data subject first.

5.3 Principle (c): Data minimisation

The School will ensure that:

- we collect personal data necessary for the relevant purposes and ensure it is not excessive
- the information we process is necessary for and proportionate to our purposes
- where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it.

5.4 Principle (d): Accuracy

The school will ensure that:

- Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay
- If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision

5.5 Principle (e): Storage limitation

The school will ensure that:

- all special category data processed by us is retained for the periods set out in our Retention Schedule
- we determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs. Our retention schedule is reviewed regularly and updated when necessary.

5.6 Principle (f): Integrity and confidentiality

The school will ensure that:

- data protection by design is at the heart of developing and maintaining our core systems and procedural developments
- all employees have completed mandatory training and receive annual refresher training in meeting their responsibilities under data protection legislation
- all of our employees are subject to confidentiality obligations with respect to personal data
- where we use data processors to process any personal data on our behalf, we have established data processing agreements
- routine data transfers that are necessary for our core school business processes are secure and use industry standard encryption methods. We regularly review our processes for data transfer in line with new technological developments.
- we have a robust IT infrastructure which has been implemented using the secure by design principle and we hold the Cyber Essentials Plus certification to guard against the most common cyber threats and demonstrate our commitment to cyber security

- hard copy information is processed in line with our security procedures
- our electronic systems and physical storage have appropriate access controls applied.

6 DUAA 2025 considerations

6.1 Children's Higher Protection Requirements.

As a school processing children's data, we are required under the DUAA 2025 to explicitly consider children's higher protection matters when determining appropriate technical and organisational measures. This means we consider:

- How children can be best protected and supported when using our services
- That children merit specific protection regarding their personal data because they may be less aware of the risks and consequences associated with certain personal data processing
- That children have different needs at different ages and stages of development

6.2 Data Subject Access Requests (DSARs)

The DUAA 2025 clarifies time limits for responding to DSARs:

- We will respond to DSARs within one month of receipt
- We will only conduct reasonable and proportionate searches when responding
- We may extend the deadline by up to two months if the request is complex or if we receive multiple requests
- If we use an extension, we will inform the data subject within the first month and explain the reason
- Where we need more information from the requester to locate or identify the data, we can pause the response time ("stop the clock") until we receive that information

6.3 Complaints Handling

Under the DUAA 2025, we are required to:

- Provide mechanisms to help individuals make complaints about our data processing, such as an electronic complaints form
- Acknowledge complaints within 30 days
- Respond to complaints without undue delay
- Inform individuals about the outcome of their complaint

6.4 Automated Decision-Making (ADM)

If we use any automated decision-making processes that have legal or similarly significant effects on individuals, we will:

- Ensure meaningful human involvement in the decision-making process
- Provide information about significant decisions made
- Enable individuals to make representations about and challenge such decisions
- Ensure individuals can obtain human intervention

6.5 International Data Transfers

When transferring personal data outside the UK, we apply the data protection test introduced by the DUAA 2025, which assesses whether the protection offered is "not materially lower" than UK GDPR standards, rather than the previous "essentially equivalent" test.

6.6 Recognised Legitimate Interests

Where we process data for certain recognised legitimate interests (such as safeguarding, crime prevention, or emergency response), we may be able to rely on this as a lawful basis without conducting a full balancing test, where this applies to our processing activities.

7 Review

7.1 The school will be responsible for ensuring that this policy is maintained and reviewed at regular intervals.

7.2 This policy will be reviewed in light of any further guidance issued by the Information Commission (formerly the ICO) regarding the DUAA 2025 amendments.

8 Other Documentation

This policy should be read in conjunction with:

- Data Protection Policy
- Records Management Policy / Records Retention and Disposal Schedule
- Data Breach Guidance
- Privacy Notices
- Complaints Handling Procedure
- Online Safety Policy