LDST
Liverpool Diocesan Schools Trust

St Michael's Church of England High School

'Jesus grew in wisdom and stature' (Luke 2:52)

DATA PROTECTION Appropriate Policy Document

Special category and criminal conviction personal data

OUR TRUST'S PRAYER

Heavenly Father

Let peace, friendship and love grow in our schools

Send the Holy Spirit to give:

Excellence to our learning

Love to our actions and

Joy to our worship

Guide us to help others

So that we may all

Learn, Love and Achieve, Together with Jesus.

Amen

Our processing of special categories of personal data and criminal offence data

As part of our functions, we process special category data and criminal offence data in accordance with the requirements of Article 9 and 10 of the UK General Data Protection Regulation ('UK GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018'). Where we refer to "the Trust" or "our Trust" within this policy, this includes all LDST schools.

1.Special category data

Special category data is defined at Article 9 UK GDPR as personal data revealing:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health; or
- Data concerning a natural person's sex life or sexual orientation

2.Criminal conviction data

Article 10 UK GDPR covers processing in relation to criminal convictions and offences or related security measures. 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'.

3.This policy document

Some of the Schedule 1 conditions for processing special category and criminal offence data require us to have an Appropriate Policy Document ('APD') in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 and policies regarding the retention and erasure of such personal data.

This document explains our processing and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018.

In addition, it provides some further information about our processing of special category and criminal offence data where a policy document isn't a specific requirement. The information supplements our privacy notices which are available on our website.

4. Conditions for processing special category and criminal offence data

When special category personal data is being processed then an additional legal ground must apply to that processing. We will normally only process special category personal data under following legal grounds:

Article 9(2)(b) - where the processing is necessary for employment law purposes, for example in relation to sickness absence;

Article 9(2)(g) - where the processing is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;

Article 9(2)(h) - where the processing is necessary for health or social care purposes, for example in relation to pupils/students with medical conditions or disabilities;

Article 9(2)(c) - there may be circumstances where it is considered necessary to process special category personal data in order to protect the vital interests of a data subject. This might include medical emergencies where the data subject is not in a position to give consent to the processing. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

Article 9(2)(a) - where none of the above apply then we will seek the consent of the data subject to the processing of their special category personal data, for example biometric fingerprints for cashless catering.

We process criminal offence data under Article 10 of the UK GDPR.

Examples of our processing of criminal offence data include pre-employment checks (DBS, barred list) and declarations by a member of our workforce in line with contractual/safeguarding obligations.

5. Processing which requires an Appropriate Policy Document

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require an Appropriate Policy Document [APD] (see Schedule 1 paragraphs 1 and 5).

This section of the policy is the APD for our Trust. It demonstrates that the processing of special category ('SC') and criminal offence ('CO') data based on these specific Schedule 1 conditions is compliant with the requirements of the UK GDPR Article 5 principles. In particular, it outlines our retention policies with respect to this data.

Description of data processed

- Health and medical data - workforce and pupils/students
- Ethnicity – pupils/students and workforce
- Religion – pupil/students and workforce
- Biometric (fingerprint) data for cashless catering, access control or library systems
- Biometric data (facial recognition) on our trust provided mobile devices (where applicable)
- Trade union membership - staff
- Criminal records - DBS checks for all members of the workforce (paid and voluntary)

Further information about this processing can be found in our privacy notices.

We also maintain a record of our processing activities in accordance with Article 30 of the UK GDPR.

Schedule 1 conditions for processing

Special Category (SC) data

We process SC data for the following purposes in Part 1 of Schedule 1:

- Paragraph 1(1) employment, social security and social protection.

We process SC data for the following purposes in Part 2 of Schedule 1. All processing is for the first listed purpose and might also be for others dependent on the context:

- Paragraph 6(1) and (2)(a) Statutory etc and government purposes
- Paragraph 8(1) and (2) Equality of opportunity or treatment
- Paragraph 18(1) Safeguarding of children and of individuals at risk

Criminal offence data

We process criminal offence data for the following purposes in parts 1 and 2 of Schedule 1:

- Paragraph 1 – employment, social security and social protection

Procedure for ensuring compliance with the principles

Accountability principle

We have put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

- The appointment of a data protection officer who reports directly to our highest management level.
- Taking a 'data protection by design and default' approach to our activities.
- Maintaining documentation of our processing activities.

- Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors.
- Implementing appropriate security measures in relation to the personal data we process.
- Carrying out data protection impact assessments for our high risk processing.

We regularly review our accountability measures and update or amend them when required.

Principle (a): lawfulness, fairness and transparency

Processing personal data must be lawful, fair and transparent. It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing meets at least one of the conditions in Schedule 1.

We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice, staff privacy notice and this policy document.

Our processing for purposes of substantial public interest is necessary to function as a school/trust under the Education Act 2005

Our processing for the purposes of employment relates to our obligations as an employer.

We also process special category personal data to comply with other obligations imposed on the school/trust by the Department for Education or our local authority.

Principle (b): purpose limitation

We process personal data for the purposes explained above when the processing is necessary for us to fulfil our statutory functions as a Trust.

If we are sharing data with another controller, we will document that they are authorised by law to process the data for their purpose.

We will not process personal data for purposes incompatible with the original purpose for which it was collected.

Principle (c): data minimisation

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.

Principle (d): accuracy

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.

Principle (e): storage limitation

All special category data processed by us for the purpose of employment or substantial public interest 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.

Principle (f): integrity and confidentiality (security)

Electronic information is processed within our secure network. Paper copies of personal data are kept locked in filing cabinets in locked offices.

Our electronic systems and physical storage have appropriate access controls applied, only relevant staff have access to the files.

The systems we use to process personal data allow us to erase or update personal data at any point in time where appropriate.

Retention and erasure policies

Our retention and erasure practices are set out in our retention schedule which is available on request from our Trust.

APD review date

This policy will be retained for the duration of our processing and for a minimum of 6 months after processing ceases. This policy will be reviewed **biennially.**

Review Schedule

Policy Author	Data Protection Officer (DPO)
Policy Approver	Board of Directors
Current Policy Version	2.1
Policy Effective From	March 2023
Policy Review Date	March 2025

Revision Schedule

Version	Revisions	By whom
1.0	Original Policy	DPO
2.0	New Policy – points 1 to 4 were not in the original policy (provides additional information regarding our Trust's processing). Point 5, which was the basis of the original policy, has been completely updated to provide more clarity. GDPR changed to UK GDPR throughout.	DPO
2.1	Reviewed March 2023 with no change	DPO