Data Protection
Appropriate Policy Document

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions outlined in Schedule 1.

This document demonstrates that the processing of SC and CO data based on these specific Schedule 1 conditions is compliant with the requirements of the General Data Protection Regulation (GDPR) Article 5 principles.

The APD is kept under review with the wider Data Protection Policy, and will be retained until six months after the date the relevant processing is stopped.

Description of data processed

The Trust processes the following SC/CO data:

- Racial or ethnic origin (staff & pupils)
- Data concerning health (staff & pupils)
- Criminal offence data (staff)
- Trade Union Membership

Schedule 1 condition for processing

- Racial or ethnic origin (staff & pupils) - Article 9 (2) (b)
- Data concerning health - Article 9 (2) (h)
- Criminal offence data - Article 9 (2) (b)

Procedures for ensuring compliance with the principles

Accountability principle
i. The Trust's processing activities are documented in the Information Asset Register, the School Information Asset Register, and the Visual Data Map.

ii. The Trust's Data Protection Policy is available to all staff, and on the website, and is reviewed every 3 years.

iii. Data Protection Impact Assessments are carried out for all new projects involving data. These are undertaken by the DPO, and reviewed by the Board.

Principle (a): lawfulness, fairness and transparency

i. The appropriate lawful basis for processing and a further Schedule 1 condition for processing SC/CO data is listed for all data processing within the Information Asset Register.

ii. Privacy notices are available for pupils/parents, job applicants, staff, volunteers, and training delegates on the Trust website, and are sent out to new parents, job applicants and staff at the relevant time.

Principle (b): purpose limitation

i. The purpose of processing SC/CO data is clearly outlined in the Information Asset Register.

ii. Appropriate details of these purposes are included in our privacy information for individuals.

iii. If we plan to use personal data for a new purpose (other than a legal obligation or function set out in law), the DPO checks that this is compatible with our original purpose. If it is not, the Trust will get specific consent for the new purpose.

Principle (c): data minimisation

i. The Trust Board is satisfied that we only collect SC/CO personal data we actually need for our specified purposes.

ii. The Trust Board is satisfied that we have sufficient SC/CO data to properly fulfil those purposes.

iii. The Trust Board is satisfied that there are processes in place to periodically review this particular SC/CO data, and delete anything we don't need.

Principle (d): accuracy

i. The Trust has appropriate processes in place to check the accuracy of the SC/CO data collected, this is outlined in the Data Protection Policy. The source of data is recorded in the Information Asset Register.

ii. The Trust has an annual process in place to update the SC/CO data to properly fulfil our purpose.

iii. The Data Protection policy outlines how we keep records of mistakes and opinions, how we deal with challenges to the accuracy of data and how we ensure compliance with the individual's right to rectification. The Data Accuracy Register records any challenges to accuracy of data held.

Principle (e): storage limitation

i. The Board has carefully considered how long we keep the SC/CO data and the justification, this is recorded in the Information Asset list and the Record Retention Schedule. This is reviewed in line with our policy schedule.

ii. Information is reviewed annually, and SC/CO data is erased in line with the Retention Schedule.

iii. SC/CO data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes is clearly identified in the Privacy Notices.

Principle (f): integrity and confidentiality (security)

i. The risks presented by our processing has been analysed in the Information Asset list, and this is used to assess the appropriate level of security we need for this data.

ii. The Trust has a cyber security policy which incorporated protection of this SC/CO data. It is the Head's responsibility to make sure the policy is implemented, and the DPO reports this to the Board. It is regularly reviewed in line with the policy schedule.

iii. Cyber security technical measures or controls are in place to protect the SC/CO data we are processing.

Retention and erasure policies

Retention and erasure procedures are contained in the Trust's Retention Schedule.