AGAPE
MULTI ACADEMY TRUST

# 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.

This document will demonstrate 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. In particular, it will outline our retention policies with respect to this data. (See Schedule 1 Part 4).

As we process SC or CO data for a number of different purposes we do not need a separate policy document for each condition or processing activity – this document covers them all. We may reference policies and procedures which are relevant to all the identified processing. Whilst we may explain our compliance with the principles in general terms, without specific reference to each individual Schedule 1 condition we have listed, we will provide the data subject with sufficient information to understand how we are processing their SC or CO data and how long we will retain it for.

However if we rely on one of these conditions, our general record of processing activities under GDPR Article 30 must include:

(a) the condition which is relied upon;
(b) how the processing satisfies Article 6 of the GDPR (lawfulness of processing); and
(c) whether the personal data is retained and erased in accordance with the retention policies outlined in this APD, and if not, the reasons why these policies have not been followed.

This document therefore complements our general record of processing under Article 30 of the GDPR and provides SC and CO data with further protection and accountability. See Schedule 1 Part 4 paragraph 41.

We will keep the APD under review and will retain it until six months after the date we stop the relevant processing. If the Information Commissioner asks to see it, we will provide it free of charge.

## Description of data processed

- Health data (pupils, parents (only where relevant to the pastoral care of their child) and workforce)
- Religious beliefs data (pupils and members, trustees and governors (only where it is relevant to an application to join the Trust Board or Local Governing Committee))
- Ethnicity data (pupils and workforce)
- Criminal offence data (workforce and members, trustees and governors via an enhanced DBS check. Pupils – added onto CPOMS only)
- Trade Union membership (workforce)

## Schedule 1 condition for processing

Give the name and paragraph number of your relevant Schedule 1 condition(s) for processing. Alternatively, you may wish to provide a link to your privacy policy, your record of processing or any other relevant documentation:

Please refer to our privacy notices on our website for:

- Pupils/parents & carers
- Workforce
- Members, Trustees & Governors
- Third parties

## Procedures for ensuring compliance with the principles

**Accountability principle**

i. Do we maintain appropriate documentation of our processing activities?
ii. Do we have appropriate data protection policies?
iii. Do we carry out data protection impact assessments (DPIA) for uses of personal data that are likely to result in high risk to individuals' interests?

Yes, we have the following policies/documents which are regularly reviewed:

- Data protection policy
- Records retention schedule
- CCTV policy
- Acceptable use policy
- Staff code of conduct

All of our Data Protection Officers report to the highest management level.

**Principle (a): lawfulness, fairness and transparency**

i. Have we identified an appropriate lawful basis for processing and a further Schedule 1 condition for processing SC/CO data?
ii. Do we make appropriate privacy information available with respect to the SC/CO data?
iii. Are we open and honest when we collect the SC/CO data and do we ensure we do not deceive or mislead people about its use?

Yes, via the privacy notices published on our website which are regularly reviewed.

On 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 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 the Trust. This has been approved by Trustees and communicated to all stakeholders by publishing on the Trust and School websites.

**Principle (b): purpose limitation**

i. Have we clearly identified our purpose(s) for processing the SC/CO data?
ii. Have we included appropriate details of these purposes 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), do we check that this is compatible with our original purpose or get specific consent for the new purpose?

Yes – please refer to the privacy notices.

**Principle (c): data minimisation**

i. Are we satisfied that we only collect SC/CO personal data we actually need for our specified purposes?
ii. Are we satisfied that we have sufficient SC/CO data to properly fulfil those purposes?
iii. Do we periodically review this particular SC/CO data, and delete anything we don't need?

Yes, via data protection audits and review of our processes and documentation.

**Principle (d): accuracy**

i. Do we have appropriate processes in place to check the accuracy of the SC/CO data we collect, and do we record the source of that data?
ii. Do we have a process in place to identify when we need to keep the SC/CO data updated to properly fulfil our purpose, and do we update it as necessary?

iii. Do we have a policy or set of procedures which outline 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?

We collect the data directly from the data subject or in the case of pupils, their parents/carers. Data is updated as and when the data subject informs us it has changed or updated.

Challenges to the accuracy of data is contained in our data protection policy published on the Trust and individual schools' websites.

**Principle (e): storage limitation**

i. Do we carefully consider how long we keep the SC/CO data and can we justify this amount of time?
ii. Do we regularly review our information and erase or anonymise this SC/CO data when we no longer need it?
iii. Have we clearly identified any SC/CO data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes?

Yes, we have a retention schedule that is regularly reviewed to ensure we can justify the amount of time we hold the data for. Data is deleted in accordance with that schedule. We determine the retention period for data based on our legal obligations and the necessity of its retention for our business needs.

We have not identified any SC/CO data that we need to keep for public interest archiving, scientific or historical research or statistical purposes.

**Principle (f): integrity and confidentiality (security)**

i. Have we analysed the risks presented by our processing and used this to assess the appropriate level of security we need for this data?
ii. Do we have an information security policy (or equivalent) regarding this SC/CO data and do we take steps to make sure the policy is implemented? Is it regularly reviewed?
iii. Have we put other technical measures or controls in place because of the circumstances and the type of SC/CO data we are processing?

Yes, and we have an acceptable use policy that covers information security that is regularly reviewed by the school's Data Protection Officer and Network Manager. Our information security is reviewed via external audits and any required adaptations implemented. We have appropriate security measures in place and these are reviewed regularly to ensure they remain appropriate in light of technological advances.

All staff are required to have 2 factor authentication. Members of staff only have access to the parts of the network and information they need to carry out their role. This includes access to SIMS (pupil and staff data) and CPOMS (safeguarding data). Hard copies of data are stored in HR

or pupil folders which are stored in staff only members areas of the school in locked cabinets. Only a relevant member of staff has a key to the locked cupboard.

All employees have completed mandatory training and receive refresher training in meeting their responsibilities under data protection legislation

All of our employees and trustees/governors are subject to confidentiality obligations with respect to personal data.

We regularly review our processes for data transfer in line with new technological developments.

We have a robust IT infrastructure to guard against the most common cyber threats and demonstrate our commitment to cyber security via annual training and cyber security external audits.

## Retention and erasure policies

You need to explain your retention and erasure policies with respect to each category of SC/CO data (this could include a link to your retention policy if you have one). You need to explicitly indicate how long you are likely to retain each specific category of SC/CO data.

Our retention schedule is available upon request from the respective school's office.

## APD review date

Every 3 years or earlier if required.