Sidney Stringer
Multi Academy Trust

Data Protection Policy

September 2014 – May 2018

Policy Due for Review in May 2018
(To Ensure Full Compliance with GDPR)

Person Responsible: Assistant Principal for ICT (MAT)

Principles

The Multi Academy Trust has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

The Multi Academy Trust intends to comply fully with the requirements and principles of the Data Protection Act 1984, the Data Protection Act 1998 and the General Data Protection Regulation (2018). All members of staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines**.**

Enquiries

Information about the the Data Protection Policy for any school within the Sidney Stringer Multi Academy Trust is available from the Assistant Principal for ICT (MAT). General information about the Data Protection Act can be obtained from the Data Protection Commissioner (Information Line 08456 306060 or 01625 545 745 or website www.ico.gov.uk).

Fair Obtaining and Processing

The Sidney Stringer Multi Academy Trust undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data are held, the likely recipients of the data and the data subjects' right of access. Information about the use of personal data is printed on the appropriate collection form. If details are given verbally, the person collecting will explain the issues before obtaining the information.

Processing means obtaining, recording or holding the information or data or carrying out any set of operations on the information or data.

Data subject means an individual who is the subject of personal data or the person to whom the information relates.

Personal data means data, which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, along with names and photographs if published in the press, Internet or media. However, this policy recognises that personal data can be any data attached to an individual.

Parent has the meaning given in the Education Act 1996, and includes any person having parental responsibility or care of a child.

Registered Purposes

The Data Protection Registration entries for schools within the Sidney Stringer Multi Academy Trust can be requested for inspection upon appointment. Explanation of any codes and categories entered is available from the Business & Finance Manager. The Assistant Principal for ICT (MAT) is the person nominated to deal with data protection issues in the Trust. Registered purposes covering the data held at the school are listed on the school's registration and data collection documents. Information held for these stated purposes will not be used for any other purpose without the data subject's consent**.**

Data Integrity

The Academy undertakes to ensure data integrity by the following methods:

Data accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the Academy of a change of circumstances their computer record will be updated as soon as is practicable. A printout of their data record will be provided to data subjects every twelve months so they can check its accuracy and make any amendments.

Where a data subject challenges the accuracy of their data, Academies will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Academy's Governing Body for their judgement. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

Data adequacy and relevance

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. It will be handled legally, fairly and Academies will be transparent in their use of data with subjects. In order to ensure compliance with this principle, Academies will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

Length of time

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the Assistant Principal for ICT (MAT) to ensure that obsolete data is properly erased**.**

Subject access

The Data Protection Acts, and the upcoming General Data Protection Regulation (2018), extend to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Where a request for subject access is received from a pupil, the school's policy is that:

- Requests from pupils will be processed as any subject access request as outlined below and the copy will be given directly to the pupil, unless it is clear that the pupil does not understand the nature of the request.

- Requests from pupils who do not appear to understand the nature of the request will be referred to their parents or carers.

- Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.

Processing subject access requests

Requests for access must be made in writing.

Pupils, parents or staff may ask for a Data Subject Access form (Appendix A). Completed forms should be submitted to the Principal of an Academy within the Sidney Stringer Multi Academy Trust. Provided that there is sufficient information to process the request, a record will be made showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (e.g. Student Record, Personnel Record), and the planned date of supplying the information (normally not more than 40 days from the request date). Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided.

Note: In the case of any written request from a parent regarding their own child's record, access to the record will be provided within 15 school dates in accordance with the current Education (Pupil Information) Regulations.

Authorised disclosures

Academies will, in general, only disclose data about individuals with their consent. However there are circumstances under which the authorised Data Protection Officer for each Academy may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- Pupil data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations.
- Pupil data disclosed to authorised recipients in respect of their child's health, safety and welfare.
- Pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school.
- Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.
- Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the academy. Officers and IT personnel writing on behalf of the Local Authority are IT liaison/data processing officers, for example in the LA, are contractually bound not to disclose personal data.

Only authorised and trained members of staff are allowed to make external disclosures of personal data. Data used within academies by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the school who needs to know the information in order to do their work. The school will not disclose anything on pupils' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything where suggests that they are, or have been, either the subject of or at risk of child abuse.

A "legal disclosure" is the release of personal information from the computer to someone who requires the information to do his or her job within or for the school, provided that the purpose of that information has been registered.

An “illegal disclosure” is the release of information to someone who does not need it, or has no right to it, or one which falls outside the School’s registered purposes.

Data and Computer Security

The Sidney Stringer Multi Academy Trust undertakes to ensure security of personal data held in electronic and physical systems by the following general methods:

Physical security

Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks. Only authorised persons are allowed in server rooms that store sensitive information. Disks, tapes and printouts are locked away securely when not in use. Visitors to schools within the Trust are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied**.**

Logical security

Security software is installed on all computers containing personal data. The Trust only shares or grants access to files that users require for their role. Computer files, stored both on internal and core external services, are backed up regularly and stored securely.

Procedural security

In order to be given authorised access to the computer, staff will have to undergo checks and will sign a confidentiality agreement. All members of staff are trained in their data protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal.

Overall security policy for data is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent.

Any queries or concerns about security of data in the school should in the first instance be referred to the Assistant Principal for ICT (MAT).

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

Data Stored in External Services

Where any personal data is stored by external agencies, companies or services required by the Sidney Stringer

Multi Academy Trust will ensure that it is held in compliance with the General Data Protection Regulation (2018). Users will be made fully aware of the data that has been stored in any external service.

The Sidney Stringer Multi Academy Trust does recognise that data stored in Google Suite may travel outside of the European Union (EU). Based on DfE guidance and Google's self-certification we accept that this is handled safely and securely within the UK-US Privacy Shield.

Appendix A - Access to Personal Data Request

DATA PROTECTION ACT 1998
Section 7

ENQUIRER DETAILS	
Name:	
Address:	
Daytime telephone number:	Evening telephone number:

DETAILS OF THE ENQUIRY

Are you the person who is the subject of the records you are enquiring about (i.e. the "Data Subject")?

Yes No

☐ **If NO,** ☐
Do you have parental responsibility for a child who is the "Data Subject" of records you are enquiring about?

Yes No

☐ **If YES,** ☐

Name of child or children about whose personal data records you are enquiring:

……..……...

Description of concern / area of concern:

……..……...

……..……...

Description of information or topic(s) requested (in your own words):

……..……...

……..……...

……..……...

……..……...

ADDITIONAL INFORMATION
Please despatch reply to (if different from enquirer's details as stated on this form):

Name:
Address:

DATA SUBJECT DECLARATION **I request that the academy search it's records based on the information supplied above under Section 7 (1) of the Data Protection Act 1998 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the academy.** **I agree that the reply period will commence when I have supplied sufficient information to enable the academy to perform the search.** **I consent to the reply being disclosed and sent to me at my stated address (or to the despatch name and address above who I have authorised to receive such information).**	
Signature of "Data Subject" (or Subject's Parent):	Date:
Name of "Data Subject" (or Subject's Parent): (PRINTED)	