Data Protection (GDPR) Policy

This policy applies across all partner schools in the Stephen Sutton Multi-Academy Trust (SSMAT). It is available on the SSMAT website and is accessible from our schools' websites.

POLICY APPROVAL and REVIEW

Review date: ***Mar. '18***

Approval needed by: ***Finance, Audit and Risk Committee***

Adopted: ***Apr. '18***

Next review date: ***Apr. '20***

CONTENTS:

1. Introduction / Overview

1.1 Stephen Sutton Multi-Academy Trust (SSMAT) is required to keep and process certain information about its staff members and students, in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

1.2 SSMAT and its schools may, from time to time, be required to share personal information about staff or students with other organisations, including other schools, educational bodies, the police and social services.

1.3 This policy is in place in order to provide a framework through which staff, governors and directors are aware of their responsibilities, and in order to outline how SSMAT and its schools comply with the core principles of the GDPR.

1.4 Organisational methods for keeping data secure are of prime importance, and SSMAT believes that it is good practice to keep policies uncomplicated, backed up by written procedures.

1.5 This policy complies with the requirements set out in the GDPR (effective from 25 May 2018) and should be read in conjunction with the SSMAT Records Management (GDPR) Policy and the Trust's Privacy Notices (which are included in the Appendix).

2. Key people

2.1 Under the terms of the GDPR, organisations are required to clarify who, in practice, takes the role of Controller (with regards to data management and protection). A Controller determines the purposes and means of processing personal data. In SSMAT, this responsibility is undertaken by the Executive Director (on behalf of the Trust Board).

2.2 The Data Protection Officer (DPO) provides advice and guidance and monitors compliance across the Trust, reporting to the Controller and, as appropriate, communicating directly with the Information Commissioner's Office (ICO).

2.3 The Controller nominates a Representative in each SSMAT partner school, who is responsible for ensuring that the Trust's Data Protection (GDPR) Policy is implemented consistently and effectively. This will generally be the Headteacher of the school.

2.4 The Headteacher of each partner school nominates a Data Protection Lead (DPL), for that school, who (on a managerial/operational basis) organises and oversees implementation (with advice and support from the DPO).

2.5 Throughout SSMAT and its schools there will be a variety of Processors, who are responsible for processing personal data on behalf of the Controller (and the relevant Representative).

2.6 Appendix 1 lists the colleagues (by name) who have specific named responsibilities for the GDPR and their contact details.

3. Legal framework

3.1 This policy has due regard to legislation, including (but not limited to):

- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

3.2 The policy also has regard to:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) - 12 steps to take now'

4. Applicable data

4.1 For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and 'pseudonymised'[1] data, e.g. key-codes.

4.2 There are higher levels of expectation in relation to more sensitive data, under the 1998 Data Protection Act. Sensitive personal data is defined, under the GDPR, as data relating to 'special categories', namely:

- race;
- ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; and
- sexual orientation.

[1] Pseudonymisation is the separation of data from direct identifiers, so that a linkage to an identity is not possible without additional information that is held separately. *(International Association of Privacy Professionals, 2018)*

5. Principles

5.1 In accordance with the requirements outlined in the GDPR, personal data is:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;[2]
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up-to-date[3];
- kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed[4]; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5.2 The GDPR also requires that: '… the Controller shall be responsible for, and able to demonstrate, compliance with the principles".

6. Accountability

6.1 SSMAT and its schools implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

6.2 Comprehensive, clear and transparent privacy procedures are in place.

6.3 Records of activities relating to higher risk processing are maintained, including the processing of 'special categories' data and data that relates to criminal convictions and offences.

6.4 Internal records of processing activities include:

- categories of personal data and data subjects;
- purpose(s) of the processing;

[2] Further processing, for archiving purposes, in the public interest, for scientific or historical research purposes or for statistical purposes shall not be considered to be incompatible with the initial purposes.

[3] Every reasonable step must be taken to ensure that personal data that is inaccurate (having regard to the purposes for which they are processed) is erased, or rectified, without delay.

[4] Personal data may be stored for longer periods, in so far as the personal data is processed solely for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

- details of recipients to whom the data will be disclosed;
- details of transfers to third parties, including documentation of the transfer mechanism safeguards in place.
- retention schedules; and
- a description of technical and organisational security measures.

6.5 SSMAT and its schools implement necessary and sufficient measures that meet the principles of data protection, including:

- data minimisation;
- pseudonymisation;
- transparency;
- allowing individuals to monitor processing; and
- continuously creating and improving security features.

6.6 Data protection impact assessments will be used, as appropriate.

7. Data Protection Officer (DPO) role

7.1 The key roles of the DPO are to:

- inform and advise colleagues of their obligations to comply with the GDPR and other data protection laws; and to
- monitor compliance with the GDPR and associated laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

7.2 The role of DPO is undertaken by the Trust Business Manager (TBM), whose other duties must not lead to a conflict of interests.

7.3 The DPO has the professional experience and knowledge of data protection law, particularly in relation to schools, and will undertake all necessary training to prepare them fully for the role.

7.4 The DPO reports to the Controller (highest level of management), who is the Trust's Executive Director.

7.5 The DPO operates independently and will not be penalised for exercising the responsibilities attached to the post.

7.6 Sufficient resources are provided, by the Trust, in order that the DPO is able to meet their GDPR obligations.

8. Lawful processing

8.1 The legal basis for processing data is identified and documented, prior to the processing of the data.

8.2 Under the GDPR, data is lawfully processed when:

- processing is necessary for:
  - compliance with a legal obligation;
  - the performance of a task carried out in the public interest;
  - the exercise of official authority that has been vested in the Controller;
  - the performance of a contract with the data subject (or to take steps to enter into a contract);
  - protecting the vital interests of a data subject, or another person; or
  - the purposes of legitimate interests pursued by the Controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject; or when:

- the consent of the data subject has been obtained.

8.3 Sensitive data is only processed when:

- the data subject has given consent explicitly (unless reliance on consent is prohibited by EU or UK law);
- the processing is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim, provided that the processing relates only to members, or former members, of the organisation (or those who have regular contact with it, in connection with those purposes) and provided there is no disclosure to a third party without consent;
- it relates to personal data that is made public (manifestly) by the data subject; or
- it is necessary for:
  - carrying out obligations under employment, social security or social protection law, or conditions that relate to a collective agreement;
  - protecting the vital interests of a data subject, or another individual, where the data subject is physically, or legally, incapable of giving consent;
  - the establishment, exercise or defence of legal claims, or where courts are acting in their judicial capacity.
  - reasons of substantial public interest (on the basis of EU or UK law) proportionate to the aim pursued and containing appropriate safeguards;
  - the purposes of preventative or occupational medicine, for assessing the working capacity of a colleague, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems

and services (on the basis of EU or UK law, or a contract with a health professional);

— reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices; or

— archiving purposes that are in the public interest, or for scientific and historical research purposes or statistical purposes (in accordance with Article 89(1)).

9. Consent

9.1 Article 6(1)(b) of the GDPR gives employers a lawful basis for processing employee data, where 'processing is necessary for the performance of a contract, to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract'. Therefore, explicit consent is not required for activities that are necessary in order for the employer to support the fulfilment of its employees' contracts. However, in other circumstances, where consent is sought, and used, as the basis for data processing, certain principles must be observed:

- Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.
- Consent is only accepted where it is: given freely; specific; informed; and an unambiguous indication of the individual's wishes.
- Where consent is given, a record is kept, documenting how and when the consent was given.
- Consent can be withdrawn by an individual at any time.

9.2 SSMAT and its schools ensure that consent mechanisms meet the standards of the GDPR. Where the standard of consent is not met, an alternative legal basis for processing the data is found, or else the processing ceases.

9.3 Consent that was accepted under the Data Protection Act (DPA) is reviewed to ensure that it meets the standards of the GDPR. Acceptable consent obtained under the DPA is not obtained again.

9.4 Parental consent[5] is sought prior to the processing of a child's data, except where the processing relates to preventative or counselling services that are offered directly to a child.

[55] When relying on consent as the lawful basis for processing personal data, when offering an online service directly to a child, only children aged 13 or over are able provide their own consent. (This is the age that is proposed in the Data Protection Bill and is subject to Parliamentary approval).

10. Right to be informed / Privacy Notices (included in the Appendix)

10.1 The Privacy Notice supplied to individuals, with regard to the processing of their personal data, is written in clear, plain language so that it is concise and transparent. The Notice is easily accessible and free of charge.

10.2 Where services are offered directly to a child, the school concerned ensures that the Privacy Notice is written in a form that the child will understand.

10.3 In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information is supplied within the Privacy Notice:

- the identity and contact details of the Controller (and, where applicable, the Controller's school-based representative) and the DPO;
- the purpose of, and legal basis for, processing the data;
- the legitimate interests of the Controller, or third party;
- any recipient(s), or categories of recipient, of the personal data;
- details of transfers to third world countries and the safeguards in place;
- the retention period, or the criteria used to determine the retention period;
- the existence of the data subject's rights, including the right to:
  - withdraw consent at any time; and/or
  - lodge a complaint with a supervisory authority; and
- the existence, as applicable, of any automated decision-making, including: profiling; how decisions are made; the significance of the process; and the consequences.

10.4 Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement is provided, together with the details of the categories of personal data. Any possible consequences of failing to provide the personal data are also outlined.

10.5 Where data is not obtained directly from the data subject, information regarding the source of the personal data and whether it came from publicly accessible sources, is provided.

10.6 For data obtained directly from the data subject, the information in 10.3 is supplied at the time that the data is obtained.

10.7 In relation to data that is not obtained directly from the data subject, the information in 9.3 is supplied within one month of having obtained the data.

10.8 If disclosure to another recipient is envisaged, then the information is provided before the data is disclosed.

10.9 If the data is used to communicate with the individual, the information in 10.3 is provided when the first communication takes place.

11. Right of access / Subject Access Request (SAR)

11.1 Individuals have the right to obtain confirmation that their data is being processed.

11.2 In order to verify the lawfulness of the data processing, individuals have the right to submit a Subject Access Request (SAR) to gain access to their personal data. It is not compulsory to use this form to make a request for personal data, but the form is designed to make it easier for the school to recognise a subject access request and to make it easier for the applicant to include all the details that might be needed in order to locate the information requested. Alternatively, a SAR can be made by letter or email, to the Data Protection Officer. Contact details for the DPO (and the SAR form itself) are available in the Appendix to this policy and on the Trust and school websites.

11.3 The identity of the person making the request is verified before supplying any information.

11.4 Under the right of subject access, individuals are entitled only to their own personal data, and not to information relating to other people (unless they are acting on another individual's behalf). Subject access provides an individual with a right to see the information contained in personal data, rather than a right to see the documents that include that information.

11.5 For a Subject Access Request (SAR) to be valid, it must be made in writing. Where an applicant has a disability that makes it difficult a Subject Access Request to be made in writing, a verbal request for information is treated as though it were a valid subject access request and, as required, a response is made in a format that is accessible to the disabled person, such as Braille, large print, email or audio formats.

11.6 Responding to a Subject Access Request may involve providing information that relates both to the individual concerned and someone else. The school may not comply with the request if to do so would mean disclosing information about another individual who can be identified from that information, except where the other individual has consented to the disclosure, or it is reasonable, in all the circumstances, to comply with the request without that individual's consent.

11.7 Individuals are entitled to make a subject access request via a third party. In these cases, the school will need to be satisfied that the third party making the request is entitled to act on the individual's behalf, but it is the third party's responsibility to provide evidence that they have been given authorisation by the person concerned.

11.8 Before responding to a subject access request for information held about a child, the school will consider whether the child is mature enough to understand their rights. If there is confidence that the child can understand their rights, then (consistent with the Data Protection Act) the response will be to the child, rather than the parent. What matters is that the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so.

11.9 A copy of the information is generally supplied to the individual free of charge. A 'reasonable fee' may be charged in order to comply with requests for further copies of the

same information, or where a request is manifestly unfounded or excessive. Fees will be based on the administrative cost of providing the information.

11.10 Where a SAR has been made electronically, the information is provided in a commonly used electronic format.

11.11 Responses to requests are done without delay and, at the latest, within forty days of receipt.

11.12 In order to assist with the data search, applicants are asked to provide as much detail as possible. Guidance from the Information Commissioner Office states that: 'Data subjects frequently make open ended requests for access ('Give me a copy of all the data you hold on me'). However, the Act [Section 7(3)] specifies that a data controller is not obliged to comply with a request . . . unless he is supplied with such information as he may reasonably require in order to locate the information which that person seeks. Open-ended requests will not generally satisfy this provision'.

11.13 In the event of numerous or complex requests, the period of compliance is extended by a further two months. The individual is informed of this extension, and receives an explanation of why the extension is necessary, within one month of the receipt of the request.

11.14 Where a request is manifestly unfounded or excessive, SSMAT and its schools hold the right to refuse to respond to the request. Within forty days of the receipt of the request, the individual is informed of this decision, and the reasoning behind it, as well as their right to complain to the supervisory authority and/or to seek a judicial remedy.

11.15 In the event that a large quantity of information is being processed about an individual, the school asks the individual to specify to which request the information refers.

12. Right to rectification

12.1 Individuals are entitled to have any inaccurate or incomplete personal data rectified.

12.2 Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.

12.3 Where appropriate, the school informs the individual about the third parties to whom the data has been disclosed.

12.4 Responses to requests for rectification take place within one month, extended by two months where the request for rectification is complex.

12.5 Where no action is being taken in response to a request for rectification, the reason for this will be explained to the individual, who will also be informed of their right to complain to the supervisory authority and to seek a judicial remedy.

13. Right to erasure

13.1 Individuals hold the right to request the deletion or removal of personal data, where there is no compelling reason for its continued processing.

13.2 Individuals have the right to erasure where:

- the personal data is no longer necessary, in relation to the purpose for which it was originally collected/processed;
- the individual withdraws their consent;
- the individual objects to the processing and there is no overriding legitimate interest for continuing the processing;
- the personal data was unlawfully processed;
- the personal data must be erased in order to comply with a legal obligation; or
- the personal data is processed in relation to the offer of 'information society services'[6] to a child.

13.3 SSMAT and its schools have the right to refuse a request for erasure, where the personal data is being processed:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority;
- for public health purposes that are in the public interest;
- for archiving purposes that are in the public interest - scientific research, historical research or statistical purposes; or
- in the exercise, or defence, of legal claims.

13.4 As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention is given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

13.5 Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

13.6 Where personal data has been made public within an online environment, other organisations who process the personal data will be informed, in order to erase links to, and copies of, the personal data in question.

[6] Services normally provided for remuneration, at a distance, by means of electronic equipment, for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service. *(Thomson Reuters, Practical Law, 2018)*

14. Right to restrict processing

14.1 Individuals have the right to block or suppress the processing of personal data.

14.2 In the event that processing is restricted, SSMAT and its schools store the personal data, but do not process it further, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

14.3 The processing of personal data is restricted where:

- an individual contests the accuracy of the personal data, processing is restricted until the school has verified the accuracy of the data;
- an individual has objected to the processing and consideration is being given as to whether there are legitimate grounds for processing that override those of the individual;
- processing is unlawful and the individual opposes erasure and requests restriction instead; or
- the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

14.4 In circumstances where the personal data in question has been disclosed to third parties, these parties are informed about the restriction on the processing of the personal data, unless such a task is impossible or involves disproportionate effort to do so.

14.5 Individuals are informed when a restriction on processing has been lifted.

15. Right to data portability

15.1 Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

15.2 It should be possible to copy or transfer personal data easily from one IT environment to another in a safe and secure manner, without hindrance to usability.

15.3 The right to data portability only applies:

- to personal data that an individual has provided to a Controller;
- where the processing is based on the individual's consent, or for the performance of a contract; and
- when processing is carried out by automated means.

15.4 Personal data is provided in a structured, commonly used and machine-readable form.

15.5 Information is provided free of charge.

15.6 Where feasible, data is transmitted directly to another organisation at the request of the individual.

15.7 SSMAT and its schools are not required to adopt or maintain processing systems that are technically compatible with other organisations.

15.8 In the event that personal data concerns more than one individual, consideration is given as to whether providing the information would prejudice the rights of any other individual.

15.9 Responses to requests for portability are made within one month of receipt of the request (notwithstanding 15.10, below).

15.10 Where a request is complex, or a number of requests are received, the timeframe for response can be extended by two months, but (within one month of the receipt of the request) the individual making the request must be informed of the extension and the reasoning behind it.

15.11 Where no action is being taken in response to a request, without delay and at the latest within one month, this is communicated to the individual, explaining the reason for this and informing them of their right to complain to the supervisory authority and to seek a judicial remedy.

16. Right to object

16.1 At the first point of communication, individuals are informed of their right to object, and this information is outlined in the Privacy Notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

16.2 Individuals have the right to object to:

- processing, based on legitimate interests or the performance of a task in the public interest;
- direct marketing; and
- processing for purposes of scientific or historical research and statistics.

16.3 Where personal data is processed for the performance of a legal task or based on legitimate interests, an individual's grounds for objecting must relate to his or her particular situation. Processing of the individual's personal data will cease, unless the processing is for the establishment, exercise or defence of legal claims, or where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

16.4 Where personal data is processed for direct marketing purposes, the processing of personal data for direct marketing purposes will cease, with immediate effect, as soon as an objection is received. There is no basis for refusing an individual's objection regarding data that is being processed for direct marketing purposes.

16.5 Where personal data is processed for research purposes, the individual must have grounds relating to their particular situation, in order to exercise their right to object. Where the processing of personal data is necessary for the performance of a public interest task, there is no requirement to comply with an objection to the processing of the data.

16.6 Where the processing activity is as outlined above, but is carried out online, the school will offer a method for individuals to object online.

17. Privacy by design and Data Protection Impact Assessments (DPIAs)

17.1 SSMAT and its schools act in accordance with the GDPR by adopting a 'privacy by design' approach and by implementing technical and organisational measures that demonstrate how good data protection practice has been integrated into processing activities.

17.2 Data Protection Impact Assessments (DPIAs) are used to identify the most effective methods of complying with data protection obligations and meeting individuals' expectations of privacy.

17.3 DPIAs facilitate the identification and resolution of problems at an early stage, thus reducing associated costs and preventing reputational damage from being caused to SSMAT and its schools.

17.4 A DPIA is used when using new technologies, or when the processing is likely to result in a high risk to the rights and freedoms of individuals. High risk processing includes, but is not limited to:

- systematic and extensive processing activities, such as profiling; and
- large scale processing of special categories of data or personal data that relates to criminal convictions or offences.

17.5 DPIAs include:

- a description of the processing operations and the purposes of the processing;
- an assessment of the necessity and proportionality of the processing in relation to the purpose;
- an outline of the risks to individuals; and
- the measures to be implemented in order to address the risk.

17.6 Where a DPIA indicates high risk data processing, the Information Commissioner's Office (ICO) is consulted as to whether the processing operation complies with the GDPR.

18. Data breaches

18.1 The term 'personal data breach' refers to a breach of security that has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

18.2 The Headteacher of each SSMAT school ensures that all staff members are made aware of, and understand (through the programme of continuous professional development and training), what constitutes a data breach.

18.3 Data breaches are reported to the Controller (the Executive Director of the Trust) – contact details are found in Appendix 1 of this policy.

18.3 Where a breach is likely to result in a risk to the rights and freedoms of individuals, the Controller informs the information Commissioner's Office. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

18.4 All notifiable breaches are reported to the Information Commissioner's Office within 72 hours of the school becoming aware of it. In order to meet this requirement, data breaches are notified to the Controller without delay and, in all cases, within 24 hours of the breach. Contact details can be found in Appendix 1 of this policy. Where a breach occurs out of working hours, or at the end of a working day (especially on a Friday), notification should be made by email, leaving a contact telephone number.

18.5 The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, is assessed on a case-by-case basis.

18.6 In the event that a breach is highly likely to result in a risk to the rights and freedoms of an individual, the school will notify those concerned directly.

18.7 In the event that a breach is sufficiently serious, the public are notified without undue delay.

18.8 Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

18.9 Within a breach notification, the following information will be outlined:

- the nature of the personal data breach, including the categories and approximate number of individuals and records concerned;
- the name and contact details of the DPO;
- an explanation of the likely consequences of the personal data breach;
- a description of the proposed measures to be taken to deal with the personal data breach; and
- (where appropriate) a description of the measures taken to mitigate any possible adverse effects.

18.10 Failure to report a breach when required to do so will result in a fine, as well as a fine for the breach itself.

19. Data security

19.1 Colleagues implement a 'clear desk policy', in order to avoid unauthorised access to physical records containing sensitive or personal information. All confidential information is stored in a securely locked filing cabinet, drawer or safe with restricted access. They are not left unattended or in clear view of anywhere where there is general access. Visitors are

not allowed access to confidential or personal information. Visitors to areas that contain sensitive information are supervised at all times.

19.2 Digital data is encrypted, whilst in storage. No personally identifiable data remains on generally accessible or multi-user machines, once a user logs out.

19.3 Personal information is not stored on any form of removable storage (e.g. CD, DVD, USB memory stick, memory card, external hard drive or 'Cloud' storage).

19.4 All electronic devices are protected by either password, personal identification number (PIN) or biometric recognition system, in order to protect the information on the device, in case of theft.

19.5 Where possible, the school enables electronic devices to allow the remote blocking or deletion of data, in case of theft.

19.6 Staff do not use their personal laptops or computers for school purposes.

19.7 Communications with governors and directors (and documentation attached) do not include 'applicable data', and other correspondence of a sensitive nature is handled with an enhanced level of care, including disposing of hard copies of documentation that are used in meetings.

19.8 Colleagues are provided with their own secure login and password, and computers prompt users regularly to change their password.

19.9 Internal emails are encrypted during transmission only. External emails containing sensitive or confidential information are marked as 'confidential', by the sender, in the subject bar and this automatically encrypts the email, requiring the recipient to generate a single use code, in order to access the contents of the message. The email is automatically deleted 30 days after the date sent.

19.10 Circular emails to parents are sent 'blind carbon copy' (bcc), so that email addresses are not disclosed to other recipients.

19.11 When sending confidential information by fax, colleagues check that the recipient is correct before sending.

19.12 Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

19.13 Before sharing data, colleagues ensure that:

- they are allowed to share it;
- adequate security is in place to protect it; and
- who will receive the data has been outlined in a Privacy Notice.

19.14 The physical security of each school's buildings and storage systems, and access to them, is reviewed on a termly basis. Where an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage are put in place.

19.15 SSMAT and its schools take its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

19.16 The Data Protection Officer is responsible for ensuring that continuity and recovery measures are in place in order to ensure the security of protected data.

20. Publication of information

20.1 SSMAT and its schools publish information of their websites, including:

- policies and procedures;
- annual reports; and
- financial information.

20.2 SSMAT and its schools will not publish any personal information, including photos, on their websites without the permission of the individual concerned.

20.3 When uploading information to a school (or Trust) website, colleagues take care to consider the potential of metadata[7] or deletions that could potentially be accessed from documents and/or images on the site.

21. CCTV and photography

21.1 Recording images of identifiable individuals is a form of processing personal information, and is therefore done in a manner that is consistent with data protection principles.

21.2 Students, staff and visitors are informed (via signage, notice-boards, letters/email and website) of the existence of Closed Circuit Television (CCTV) cameras and the purpose for which CCTV images are collected.

21.3 CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

21.4. CCTV footage is kept for up to six months, for security purposes; the Data Protection Officer is responsible for ensuring that the records are secure and allowing appropriate access.

21.5 SSMAT and its schools will always indicate its intention to take photographs of students and will gain permission before publishing them. In order that the Trust and its schools are in a position to use images/video footage of pupils in publications, e.g. for the school website or prospectus, or (e.g.) through recordings of school plays, advance written permission is gained for that type of usage from the parent / carer of the student. Where specific events, such as school trips, are likely to generate photographs / video recordings,

[7] A set of data that describes and gives information about other data *(Oxford Living Dictionary, 2018)*

where practicable, permission specific to that activity is sought, as part of the planning process for the activity. Where this is not possible, the more general permissions for types of usage will apply. Parents may withdraw permissions at any time.

21.6 Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

22. Biometric information

22.1 Biometric data[8] is used with care, such that there is compliance with the data protection principles set out in the Data Protection Act 1998 and The Protection of Freedoms Act 2012.

22.2 SSMAT schools notify each parent/carer of a student under the age of 18 if they wish to take, and subsequently use, the child's biometric data as part of an automated biometric recognition system[9]. As long as the child, or a parent, does not object, the written consent of only one parent is required for the information to be processed. A child does not have to object in writing, but a parent's objection must be written.

22.3 A school does not need to notify a particular parent/carer, or seek his or her consent, if the school is satisfied that:

- the parent/carer cannot be found;
- the parent lacks the mental capacity[10] to object, or to consent
- the welfare of the child requires that a particular parent is not contacted, e.g. where a child has been separated from an abusive parent, who is not be informed of the child's whereabouts; or
- where it is otherwise not reasonably practicable for a particular parent to be notified, or for his /her consent to be obtained.

22.4 Where neither of the parents of a child can be notified (for one of the reasons in 22.3), the following conditions apply:

- Where the child is being 'looked after' by a local authority, or a voluntary ('not-for-profit') organisation, the authority, or organisation is notified and their written consent obtained.
- Where the child is not 'looked after', the notification is sent to all those caring for the child and written consent it sought from at least one carer, as a prerequisite for the processing of the biometric data (subject to neither the child nor any of the carers objecting).

[8] Personal information about an individual's physical or behavioural characteristics that can be used to identify the person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements (*Protection of biometric information of children in schools and colleges, DfE, March 2018)*

[9] A system that uses technology that measures an individual's physical or behavioural characteristics, by using equipment that operates 'automatically' (i.e. electronically). Information from the individual is compared with biometric information stored in the system to see if there is a match, in order to recognise or identify the individual.

[10] Within the meaning of the Mental Capacity Act 2005

22.5 There are no circumstances in which a school can lawfully process biometric information, for the purposes of using an automated biometric recognition system, without written consent.

22.6 If a student refuses to participate (or continue to participate) in activities that involve the processing of their biometric data, this objection overrides any parental consent to their processing. Students are informed of their right to allow their biometric data to be taken/used.

22.7 Reasonable alternative arrangements are provided for students who do not use automated biometric recognition systems, either because their parents/carers have refused consent, or due to the student's own refusal to participate in the collection of their biometric data. The alternative arrangements must not results in students experiencing any disadvantage or difficulty in accessing services as a result of their non-participation in an automated biometric recognition service. Likewise, such arrangements must not place any additional burden on parents whose children are not participating in such a system.

22.8 Biometric data is stored securely, to prevent any unauthorised or unlawful use, and is not kept for any longer than necessary. It is destroyed when, for whatever reason, the individual no longer uses the system, including when he/she leaves the school, when a parent/carer withdraws consent or when the individual objects.

23. Data retention

23.1 Data is kept for no longer than is necessary. Therefore, data that is no longer required is deleted as soon as is practicable.

23.2 Some educational records relating to former students or employees may be kept for an extended period for legal reasons, or to enable the provision of references or academic transcripts.

23.3 Paper documents are shredded or pulped, and electronic memories are 'scrubbed clean' or destroyed, at the end of the retention period.

23.4 For more detail on the Trust's approach to the storage and disposal of data, please see the SSMAT Records Management (GDPR) Policy.

24. Disclosure and Barring Scheme (DBS) data

24.1 Data provided by the DBS (including through electronic communication) is handled in line with data protection legislation and is not duplicated.

24.2 Any third parties, who access DBS information, are made aware of the data protection legislation, as well as their responsibilities as a data handler.

Stuart Jones; 16/05/18

Appendix 1 - Staff with specific GDPR-related responsibilities – by name

Stephen Sutton Multi-Academy Trust Core Team

GDPR-related role	*Job title*	*Name*	*Contact details*
Data Controller	Executive Director	Stuart Jones	stuart.jones@stephensuttonmat.co.uk 01543-687311 / 01543-687310
Data Protection Officer (DPO)	Trust Business Manager	Sharon Thorp	dpo@stephensuttonmat.co.uk 01543-687310

Chase Terrace Technology College

GDPR-related role	*Job title*	*Name*	*Contact details*
Overall responsibility for GDPR implementation in CTTC	Headteacher	Tim Chamberlin	t.chamberlin@cttc.staffs.sch.uk 01543-682286
Data Protection Lead (DPL)	Business Manager (CTTC)	Selina Morgan	s.morgan@cttc.staffs.sch.uk 01543-682286

Privacy Notice for Chase Terrace Technology College

- How we use student information

This Privacy Notice is specific to Chase Terrace Technology College, but is written to be consistent with Stephen Sutton Multi-Academy Trust's Data Protection (GDPR) Policy. The Notice relates to personal, identifiable information that relates to individual students on roll at the school.

The categories of student information that the school collects, holds and shares include:

- Personal information (such as name, Unique Pupil Number (UPN) and address / contact details)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Academic achievement data
- Rewards and sanctions (including exclusions)
- Information relating to Special Educational Needs and Disabilities (where relevant)
- Any relevant medical information.

The school collects and uses this information for 'specified, explicit and legitimate purposes' in order to:

- Support students' learning
- Monitor and report on students' progress
- Provide appropriate pastoral care
- Assess the quality of its services
- Comply with the law regarding data sharing

The lawful basis on which the information is used:

The school collects and uses student information under Section 537A of the Education Act 1996 and Section 83 of the Children Act 1989. It also complies with Article 6(1)(e) and Article 9(2)(b) of the General Data Protection Regulation (GDPR). The information is processed by the school in order that it is able to exercise the official authority that is vested in it to provide an effective education for its students.

Collecting student information:

Whilst the majority of student information provided to the school is mandatory, some of it is provided on a voluntary basis. In order to comply with the General Data Protection Regulation, the school will inform parent(s)/carer(s) whether they are required to provide certain student information for the school, or whether they have a choice in this.

Storing student data:

The school holds student data until the student reaches the age of 25, after which it is disposed of securely.

Student information is shared with:

- Schools and colleges that students attend after leaving us
- Officers of the Stephen Sutton Multi-Academy Trust (SSMAT)
- Staffordshire Local Authority (who have specific responsibilities relating to admissions, SEND and safeguarding)
- The Department for Education (DfE)
- The Education and Skills Funding Agency (ESFA)
- Police
- Social Services
- Attend (attendance and educational welfare support)
- NHS (school nurse service)
- Children and Adolescent Mental Health Services (CAMHS)
- Alliance in Partnership (AiP) [catering service]
- Digital service providers (CAPITA, 4 Matrix, Oxford Analytics, Show My Homework, My Maths, Accelerated Reading)
- Examination boards
- Work experience providers
- The Bridge (pupil referral unit)
- Residential trip organisers (and insurers)

Why we share student information:

Information about our students is not shared with anyone without consent, unless the law and the Trust's policies allow the school to do so.

Student data is shared with the Department for Education (DfE) on a statutory basis (under regulation 5 of The Education (Information about Individual Pupils) (England) Regulations 2013). This data sharing underpins school funding and educational attainment policy and monitoring. To find out more about the data collection requirements placed on schools by the Department for Education (e.g. for the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

There are a broad range of other agencies with whom the school shares students data (as listed above), in order to support the effective education and welfare of the students themselves.

Youth support services:

Once our students reach the age of 13, we also pass student information to our local authority, and/or provider of youth support services, as they have responsibilities in relation to the education or training of 13-19 year olds (under section 507B of the Education Act 1996). This enables them to provide services as youth support services and careers advice.

A parent, or guardian, can request that only their child's name, address and date of birth is passed to their local authority or provider of youth support services, by informing the school. This right is transferred to the student once he/she reaches the age 16.

The school also shares certain information about students aged 16+ with the local authority, and/or provider of youth support services, given their responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996. This enables them to provide information about post-16 education and training providers, youth support services and careers advice.

For more information about services for young people, please visit the local authority website.

The National Pupil Database (NPD):

The NPD is owned and managed by the DfE and contains information about students in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources, including schools, local authorities and awarding bodies.

The school is required, by law, to provide information about our students to the DfE, as part of statutory data collections, such as the school census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information about Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The DfE may share information about our students, from the NPD, with third parties who promote the education or well-being of children in England through conducting research or analysis, producing statistics and/or providing information, advice or guidance.

The DfE has robust processes in place to ensure that the confidentiality of student data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether, or not, the DfE releases data to third parties are subject to a strict approval process and are based on a detailed assessment of: who is requesting the data; the purpose for which it is required; the level and sensitivity of the data requested: and the arrangements in place to store and handle the data.

To be granted access to student information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the DfE's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information regarding the organisations to whom the DfE has provided student information (and for what purpose), please visit the following website:
https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact the DfE go to: https://www.gov.uk/contact-dfe

Requesting access to personal data:

Under data protection legislation, parents and students have the right to request access to information about them that is held by the school. To make a request for your personal information, or to be given access to your child's educational record, please make a Subject Access Request (SAR), addressed to Sharon Thorp, the Data Protection Officer for Stephen Sutton Multi-Academy Trust (contact details below). Guidance notes and a SAR Form can be accessed from www.stephensuttonmat.co.uk or from the school's website.

Parents/carers and students also have the right to:

- Object to processing of personal data that is likely to cause, or is causing, damage or distress
- Prevent processing for the purpose of direct marketing
- Object to decisions being taken by automated means
- (In certain circumstances) have inaccurate personal data rectified, blocked, erased or destroyed
- Claim compensation for damages caused by a breach of the Data Protection regulations

Anyone having a concern about the way that their personal data (or information relating to their child) is being collected or used, should, in the first instance, be raised with the Trust's Data Protection Officer – dpo@stephensuttonmat.co.uk . Concerns can also be raised through direct contact with the Information Commissioner's Office at https://ico.org.uk/concerns

Contact:

To discuss any aspect of this Privacy Notice, please contact Sharon Thorp, Data Protection Officer

dpo@stephensuttonmat.co.uk

01543-687310

Stephen Sutton Multi-Academy Trust

Bridge Cross Rd.

Burntwood

Staffs.

WS7 2DB

Privacy Notice for Chase Terrace Technology College

- How we use employee information

This Privacy Notice is specific to Chase Terrace Technology College, but is written to be consistent with Stephen Sutton Multi-Academy Trust's Data Protection (GDPR) Policy. The Notice relates to personal, identifiable information that relates to individual employees of Chase Terrace Technology College, a partner school in Stephen Sutton Multi-Academy Trust.

The categories of employee information that the school collects, holds and shares include:

- Personal information, such as name, employee or teacher number, national insurance number and address / contact details)
- Special categories of data, including information relating to characteristics such as ethnicity, age and gender
- Contract information, such as start dates, hours worked, post, roles and salary information
- Work absence information, such as number of absences and reasons
- Qualifications (and, where relevant, subjects taught)
- Any relevant medical information.

The school collects and uses this information for 'specified, explicit and legitimate purposes' in order to:

- Enable individuals to be paid
- Enable the school, and the Trust, to develop a comprehensive picture of the workforce and how it is deployed
- Inform the development of recruitment and retention policies

The lawful basis on which the information is used:

The school collects and uses employee information under Section 537A of the Education Act 1996 and Section 83 of the Children Act 1989. It also complies with the General Data Protection Regulation (GDPR).

Employee information is collected and used under the following GDPR categories:

- Article 6 - GDPR - Public task: Processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.
- Article 9 – GDPR – Processing of special categories of personal data: Processing is necessary for the purposes of carrying out the obligations, and exercising specific rights, of the Controller or of the data subject in the field of employment and social security and social protection law, in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.; and processing is necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in their judicial capacity.

Information is also collected through the appointment process, consistent with The School Staffing (England) Regulations 2009, 12(7) and 24(7) and the School Staffing (England) (Amendment) Regulations 2013.

Collecting employee information:

Whilst the majority of employee information provided to the school is mandatory, some of it is provided on a voluntary basis. In order to comply with the General Data Protection Regulation, the school will inform employees whether they are required to provide certain personal information for the school, or whether they have a choice in this.

Storing employee data:

The school holds employee data until six years have elapsed after the date of the termination of employment, after which it is disposed of securely.

Employee information is shared with:

- Officers (and, where required, Directors) of the Stephen Sutton Multi-Academy Trust (SSMAT)
- Staffordshire Local Authority
- The Department for Education (DfE)
- The Education and Skills Funding Agency (ESFA)
- Other public sector bodies (e.g. police, social services, where there is a clear need to do so, with a sound legal basis)
- Capita (payroll provider)
- PHRP (HR consultancy advisers) (as required, in the effective implementation of Trust HR policies)

Why we share employee information:

Information about our employees is not shared with anyone without consent, unless the law and the Trust's policies allow the school to do so.

The school is required to share employee data with the Local Authority, in order that it can fulfil its statutory duties, e.g. with regard to safeguarding, and there are circumstances where it is also necessary to share employee data with other public bodies, such as the police and social services.

Personal data is also shared with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring and evaluation and is also associated with school funding and expenditure and educational attainment.

Data collection requirements:

The DfE collects and processes personal data relating to those employed by schools (including multi-academy trusts). All state-funded schools are required to submit a census submission, because it is a

statutory return, under Sections 113 and 114 of the Education Act 2005. For more information go to: https://www.gov.uk/education/data-collection-and-censuses-for-schools

The Department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England through: research and analysis; the production of statistics; and the provision of information, advice or guidance. Robust procedures are in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to this data and its use. Decisions regarding the release of personal data to third parties are subject to a strict approval process and are based on a detailed assessment of: who is requesting the data; the purpose for which it is required; the level and sensitivity of the data requested; and the arrangements in pace to store and handle the data securely. To be granted access to school workforce information, organisations must comply with the DfE's strict terms and conditions, covering the confidentiality and handling of the data, security arrangements and retention and use of the data. For more information, go to: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data . To contact the Department, go to: https://www.gov.uk/contact-dfe

Requesting access to your personal data:

Under data protection legislation, employees have the right to request access to information about them that is held by the school. To make a request for your personal information, please make a Subject Access Request (SAR), addressed to Sharon Thorp, the Data Protection Officer for Stephen Sutton Multi-Academy Trust (contact details below). Guidance notes and a SAR Form can be accessed from www.stephensuttonmat.co.uk or from the school's website.

Employees also have the right to:

- Object to processing of personal data that is likely to cause, or is causing, damage or distress
- Prevent processing for the purpose of direct marketing
- Object to decisions being taken by automated means
- (In certain circumstances) have inaccurate personal data rectified, blocked, erased or destroyed
- Claim compensation for damages caused by a breach of the Data Protection regulations

Anyone having a concern about the way that their personal data is being collected or used, should, in the first instance, raise the issue with the Trust's Data Protection Officer – dpo@stephensuttonmat.co.uk . Concerns can also be raised through direct contact with the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact:

To discuss any aspect of this Privacy Notice, please contact Sharon Thorp, Data Protection Officer

dpo@stephensuttonmat.co.uk

01543-687310

Stephen Sutton Multi-Academy Trust

Bridge Cross Rd., Burntwood, Staffs., WS7 2DB

Subject Access Request (SAR) Form

[STRICTLY PRIVATE AND CONFIDENTIAL]

This form may be used to make a Subject Access Request (SAR), under Section 7 of the Data Protection Act 1998. Please refer to the accompanying notes to assist you in the completion of this form and send your SAT, together with proof of identity, either by email to: dpo@stephensuttonmat.co.uk or by post (marked 'Strictly Private and Confidential') to: Sharon Thorp (Data Protection Officer), Stephen Sutton Multi-Academy Trust, Bridge Cross Road, Burntwood, Staffs., WS7 2DB.

<table>
<tr><td colspan="4">1. Details of Person Requesting Information</td></tr>
<tr><td>Title (Mr./Mrs./Miss/Dr. etc.):</td><td></td><td>Date of Birth:</td><td></td></tr>
<tr><td>Surname / Family Name:</td><td></td><td>Maiden Name / Former Surname(s)</td><td></td></tr>
<tr><td>Contact Telephone Number(s):</td><td></td><td>E-mail Address:</td><td></td></tr>
<tr><td>Home Address (inc. Post Code):</td><td colspan="3"></td></tr>
<tr><td>Are you the Data Subject? (i.e. are you requesting personal data about yourself?)</td><td colspan="3">YES ☐ NO ☐</td></tr>
<tr><td colspan="4">If you checked the box for 'Yes', please attach/enclose proof of identity, as detailed in the next section.</td></tr>
<tr><td rowspan="3">If you checked 'No', please complete the boxes to the right.</td><td>Relationship to the 'Data Subject':</td><td colspan="2"></td></tr>
<tr><td>Name of the Data Subject:</td><td colspan="2"></td></tr>
<tr><td>Date of Birth of the Data Subject:</td><td colspan="2"></td></tr>
<tr><td colspan="4">Also, if you checked the box for 'No', please attach documentation that supports your application to act on the Data Subject's behalf.</td></tr>
<tr><td colspan="4">2. Proof of Identity</td></tr>
<tr><td colspan="4">In order to help us to establish your identity, please submit a copy of one document from the following:
Birth Certificate Passport Full Driving Licence Photocard Driving Licence</td></tr>
<tr><td colspan="4">3. Helping Us to Find the Information</td></tr>
<tr><td colspan="4">Please use the space below to provide further details to help us to locate the information sought, including any relevant time periods, being as precise as possible.</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">4. Declaration (to be signed and dated by the applicant)</td></tr>
<tr><td colspan="4">The information that I have supplied in this application is correct.</td></tr>
<tr><td>Signature:</td><td></td><td>Date:</td><td></td></tr>
<tr><td colspan="4">Warning: Attempting to obtain personal data to which you are not entitled may be an offence, under the Data Protection Act 1998.</td></tr>
</table>

SAR Guidance Notes

1. These notes are consistent with the Data Protection Act 1998 (Section 7).

2. Under the right of subject access, you are entitled only to your own personal data, and not to information relating to other people (unless they are acting on your behalf). Subject access provides you with a right to see the information contained in personal data, rather than a right to see the documents that include that information.

3. For a Subject Access Request (SAR) to be valid, you must make it in writing. If you have a disability that makes it difficult for you to make a SAR in writing, we will treat a verbal request for information as though it were a valid subject access request and, as required, will respond in a format that is accessible to the disabled person, such as Braille, large print, email or audio formats.

4. It is not compulsory to use this SAR form to make a request for personal data, but the form is designed to make it easier for us to recognise a subject access request and make it easier for you to include all the details that might be needed in order to locate the information requested.

5. In order to assist with the data information search, please give as much detail as possible. Guidance from the Information Commissioner Office states that: 'Data subjects frequently make open ended requests for access ('Give me a copy of all the data you hold on me'). However, the Act [Section 7(3)] specifies that a data controller is not obliged to comply with a request . . . unless he is supplied with such information as he may reasonably require in order to locate the information which that person seeks. In most cases an open ended request will not satisfy this provision'.

6. Please ensure that you have signed and dated your SAR, as we will not be in a position to process your application without this.

7. We will need to verify your identity before supplying your personal data. Please, therefore, attach a copy of one of the following:
    - Birth Certificate
    - Passport
    - Full Driving Licence or Photocard Driving Licence

8. You are entitled to make a subject access request via a third party. In these cases, we will need to be satisfied that the third party making the request is entitled to act your behalf, but it is the third party's responsibility to provide evidence that they have been authorised to act on your behalf.

9. Before responding to a subject access request for information held about a child, we will consider whether the child is mature enough to understand their rights. If we are confident that the child can understand their rights, then (consistent with the Data Protection Act) we will respond to the child rather than the parent. What matters is that the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so.

10. Responding to a Subject Access Request may involve providing information that relates both to yourself and someone else. We may not comply with the request if to do so would mean disclosing information about another individual who can be identified from that information, except where the other individual has consented to the disclosure or it is reasonable in all the circumstances to comply with the request without that individual's consent.

11. We will respond to a Subject Access Request within 40 days of its receipt.