SOUTHERN ACADEMY TRUST

Data Protection Policy

Document Control Table			
Document Title	Data Protection Policy		
Author and Job Title	Alannah Carey Bates		
Version Number	V2		
Date Approved	01/05/2018		
Approved by	MB		
Date of Review	01/05/2018		
Document History			
Version	**Date**	**Author**	**Note of Revisions**
V1	01/09/2017	MB	
V2	16/04/2018	ACB	Whole document changed to reflect changes under GDPR

Contents

1. Introduction

1.1 Southern Academy Trust collects and uses certain types of personal information about staff, students, parents, volunteers and other individuals who come into contact with the Trust and its academies in order to provide education and associated functions. The Trust may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding, and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation (GDPR), Data Protection Act and other related legislation.

2. Personal information promise

2.1 Southern Academy Trust is committed to protecting the privacy and fundamental rights of the individuals whose personal data it processes. To show our commitment we adhere to the Information Commissioner's Office (ICO) personal information promise.

I, Mark Blackman (CEO), on behalf of Southern Academy Trust, promise that we will:

- Value the personal information entrusted to us and make sure we respect that trust;
- Go further than just the letter of the law when it comes to handling personal information, and adopt good practice standards;
- Consider and address the privacy risks first when we are planning to use or hold personal information in new ways, such as when introducing new systems;
- Be open with individuals about how we use their information and who we give it to;
- Make it easy for individuals to access and correct their personal information;
- Keep personal information to the minimum necessary and delete it when we no longer need it;
- Have effective safeguards in place to make sure personal information is kept securely and does not fall into the wrong hands;
- Provide training to staff who handle personal information and treat it as a disciplinary matter if they misuse or don't look after personal information properly;
- Put appropriate financial and human resources into looking after personal information to make sure we can live up to our promises; and
- Regularly check that we are living up to our promises and report on how we are doing.

_____ Dated_____

3. Data protection principles

3.1 Southern Academy Trust is required to adhere to the six principles of the GDPR. These are:

a) Personal data shall be processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency').

b) Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in any manner incompatible with those purposes. Further processing for archiving, scientific or historical research or statistical purposes is permissible ('purpose limitation').

c) Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed ('data minimisation').

d) Personal data shall be accurate and where necessary kept up to date ('accuracy').

e) Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose ('storage limitation').

f) Personal data shall be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

4. Personal data

4.1 Personal data is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. A personal identifier can constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people. Opinions, intentions and digital imagery also constitute personal data.

4.2 To process personal data lawfully and in accordance with the first data protection principle, one of the six lawful bases set out in Article 6 of the GDPR must be met. These are;

- Consent – the individual has given consent to the processing of his or her personal data for one or more specific purposes;

- Contract - processing is necessary for the performance of a contract to which the individual is party or in order to take steps at the request of the individual prior to entering into a contract;

- Compliance - processing is necessary for compliance with a legal obligation to which the Trust is subject;

- Vital interests - processing is necessary in order to protect the vital interests of the individual or of another;

- Public interest - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Trust.

- Legitimate interests - processing is necessary for the purposes of the legitimate interests of the Trust or by a third party, except where such interests are overridden by the rights and freedoms of the individual.

4.3 Special category personal data affords additional protection under the GDPR and will not be processed by the Trust or its academies unless one of the conditions in Article 9(2) of the GDPR is satisfied in addition to meeting one of the lawful bases for processing in Article 6 of the GDPR.

4.4 Special category personal data is information which identifies an individual's;

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Health (including mental health)
- Sex life or sexual orientation
- Genetic and biometric

4.5 Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

5. Protecting personal data

5.1 Southern Academy Trust will ensure that all employees have had data protection training commensurate with the level of their responsibility for processing data. In addition, the Trust will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties.

5.2 The Trust will monitor and implement where necessary appropriate technical and organisational control measures to ensure that data is secure and record this in its record of processing activities.

6. Data retention

6.1 Personal data should only be retained for as long as is necessary and in accordance with the Trust's Data Retention Schedule.

7. Privacy notices

7.1 Individuals have the 'right to be informed' under the GDPR as to what personal data of theirs is being processed and the purpose it is being processed for. The Trust will notify its 'data subjects' of how and why it processes their personal data by way of privacy notices. Any individual that the Trust or its academies collect data from shall be directed to or provided with a relevant privacy notice. Privacy notices will also be published on each school website.

8. Records

8.1 The Trust is required to maintain a record of processing activities which covers all the processing of personal data. Amongst other information, this record contains details of why the personal data is being processed, the types of individuals about which information is held, who the personal information is shared with and when personal information is transferred to countries outside the EU. This live document is available to view. (link will be inserted here)

8.2 Staff embarking on new activities of data processing or sharing of personal data with third parties should initially check the live record of data processing and if this activity has not been previously recorded, they should contact the Data Protection Officer in advance of the processing or sharing of personal data.

9. Data protection impact assessments (DPIA)

9.1 The Trust has an obligation to complete a DPIA before carrying out processing likely to result in a high risk to individuals' interests. A DPIA will ensure accountability and compliance with the GDPR with data that is a high risk to an individual's privacy. The DPIA may result in a technical or organisational measure being implemented.

9.2 For some projects the GDPR requires that a Data Protection Impact Assessment (DPIA) is carried out. The types of circumstances when this is required include: those involving processing of large amounts of personal data, where there is automatic processing/profiling, processing of special categories of personal data, or monitoring of publicly assessable areas (i.e. CCTV). The DPIA is a mechanism for identifying and examining the impact of new initiatives and putting in place measures to minimise or reduce risks.

10. Subject access requests

10.1 Individuals have the 'right to access' their personal data so that they are aware of and can verify the lawfulness of the processing. Individuals can make a 'subject access request'. A subject access request should be made to the Data Protection Officer of the Trust who will review and carryout the request in accordance with the GDPR. The contact details for the DPO are published at the end of this document.

11. Disclosure of personal data to third parties

11.1 The Trust may receive requests from third parties (i.e. those other than the data subject, the Trust, and employees of the Trust) to disclose personal data it holds about students, their parents or guardians, staff or other individuals. This information will not generally be disclosed

but there are certain circumstances when it is permissible. Any transfers of personal data must meet the data processing principles, in particular it must be lawful and fair to the individuals concerned, and it must also meet one of the conditions of processing in Article 6 of the GDPR. If no other conditions in the Article are met then consent must be obtained from the individuals concerned before any data is shared. The Trust must be satisfied that the third party is holding the personal data securely and in accordance with the GDPR. Furthermore, where a third party is processing personal data on behalf of the Trust, a written contract must be in place with the third party to ensure the requirements of the GDPR will be met by the third party and the rights of the individuals are protected.

12. Other rights afforded to individuals under the GDPR

12.1 Right to rectification – Individuals have the right to require a controller to rectify inaccuracies in personal data held about them. In some circumstances, if personal data are incomplete, an individual can require the controller to complete the data, or to record a supplementary statement.

12.2 Right to erasure - Individuals have the right to have their data erased in certain situations such as where the data are no longer required for the purpose for which they were collected, the individual withdraws consent or the information is being processed unlawfully.

12.3 Right to restrict processing - Individuals have the right to request the restriction or suppression of their personal data in some circumstances, personal data may still be stored in this instance but processing is restricted.

12.4 Right to data portability – Individuals have the right to request information about them is provided in a structured, commonly used and machine readable form so it can be sent to another data controller. This only applies to personal data that is processed by automated means (not paper records); to personal data which the data subject has provided to the controller, and only when it is being processed on the basis of consent or a contract.

12.5 Right to object – Individuals have the right to object to specific types of processing which includes processing for direct marketing. The data subject needs to demonstrate grounds for objecting to the processing relating to their particular situation except in the case of direct marketing where it is an absolute right.

13. Breaches

13.1 The Trust is responsible for ensuring appropriate and proportionate security for the personal data that we hold. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage of the data.

13.2 The Trust makes every effort to avoid personal data breaches, however, it is possible that mistakes will occur on occasions. Examples of personal data breaches include:

- Loss or theft of data or equipment

- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Unauthorised disclosure (e.g. email sent to the incorrect recipient)
- Human error
- Hacking attack

13.3 If a data protection breach occurs the Trust is required in most circumstances to report this as soon as possible to the Information Commissioner's Office, and not later than 72 hours after becoming aware of it.

13.4 If the Trust's employees become aware of a data protection breach they must report it immediately to the Data Protection Officer. It is important that the Trust develops a culture where employees understand their obligation to report a breach. The quicker a breach is reported, the faster the Trust can work to mitigate its impact.

13.5 The Trust will keep a record of 'near misses' of data breaches to analyse its systems to allow it to make necessary organisational and technical changes to prevent a future data breach.