The STAR Multi-Academy Trust

SPECIAL CATEGORY DATA POLICY

Approved by the Trust Board (FAR Committee)	1 February 2022
Review Date	February 2024

Introduction

The STAR Multi Academy Trust processes special category and criminal conviction data in the course of fulfilling its functions as a school. Schedule 1 of the Data Protection Act 2018 requires data controllers to have in place an 'appropriate policy document' where certain processing conditions apply for the processing of special categories of personal data and criminal convictions data. This policy fulfils this requirement.

This policy complements the STAR Multi Academy Trust's existing records of processing as required by Article 30 of the General Data Protection Regulation, which has been fulfilled by the creation and maintenance of an Information Asset Register. It also reinforces the Trust's existing retention and security policies, procedures and other documentation in relation to special category data.

Scope

The STAR Multi Academy Trust is committed to the protection of all special category and criminal convictions data that it processes. This policy applies to all such data whether or not an appropriate policy document is required.

Special categories of data processed

The STAR Multi Academy Trust processes the following special categories of data:

- racial or ethnic origin,
- religious or philosophical beliefs
- trade union membership
- health
- gender identity/sexual orientation
- Biometric identifier

The STAR Multi Academy Trust also processes criminal convictions data for the purposes identified below.

The STAR Multi Academy Trust relies on the following processing conditions under Article 9 of the General Data Protection Regulation and Schedule 1 of the Data Protection Act 2018 to lawfully process special category and criminal convictions data:

Purposes	Examples of use (not exhaustive)	Processing conditions
For the provision of education to pupils, including providing support to pupils who are recognised as having Special Educational Needs.	The use of special category data to identify students who require additional support.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
To ensure the safety and wellbeing of pupils	Details of safeguarding concerns held in safeguarding files. Allergy and disability information.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
Identification/ authentication	Biometric (fingerprint) school meal payments.	Article 9 (2)(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes
To monitor pupil attendance	Medical reasons for absence.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
To maintain records of successful and unsuccessful pupil admissions	Faith school prioritisation of pupils.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
For the provision of school trips	Provision of dietary requirements to third parties involved with facilitating the school trip.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
For the provision of education in respect of Looked After Children.	Details of criminal convictions in respect of a child's parents.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes.
The management of staff	Handling of disciplinary proceedings and grievances.	Article 9(2)(b) Employment, social security and social protection Schedule 1 Part 1, 1(a) Processing necessary for the purposes of carrying out obligations and exercising specific rights of the controller and or data subject in the field of employment
Recruitment and pre-employment checks	DBS certificates.	Article 9(2)(b) Employment, social security and social protection Schedule 1 Part 1, 1(a) Processing necessary for the purposes of carrying out obligations and exercising specific rights of the controller and or data subject in the field of employment.
To facilitate the functioning of the governing body	Governors will use special category data where applicable when	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes

	considering solutions to, for example, access to school for a disabled student.	
For the prevention and detection of crime	Potential special category and criminal offence data shared	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 5 (10). Preventing or detecting unlawful acts
The handling of complaints	Complaint investigations may involve reference to and use of special category/ criminal conviction data where applicable to the content and nature of the complaint.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
To fulfil legislative health and safety requirements	Staff health information for assessment of reasonable adjustments.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
Equalities monitoring	Collection of staff and student race, ethnicity and religious background.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes

Compliance with Article 5 – The Data Protection Principles

The STAR Multi Academy Trust maintains documentation and implements procedures which ensures compliance with the Data Protection Principles under Article 5 of the General Data Protection Regulation.

Document/ procedure	Principles	How document procedure aids compliance
Privacy notices	Accountability Lawfulness, fairness and transparency Purpose limitation Accuracy Storage limitation Data minimisation	The Trust publishes a suite of privacy notices which stipulate that the Trust is the 'data controller', the purposes for which the Trust processes special category data and the lawful bases we rely on to do this. This fulfils the Trust's duty to be transparent about the data that it holds, how it is processed and that the Trust as the data controller is accountable. All privacy notices provide details of how to make a data rights request, ensuring that data subjects are able to check and challenge the lawfulness and accuracy of the data processed. Privacy notices are updated where the Trust makes changes to the way it processes personal data.

Policies	Accountability Purpose limitation Storage limitation Security Accuracy Data Minimisation	The Trust maintains a framework of information governance policies which detail the expectations and responsibilities of employees of the Trust. This includes, but is not limited to, the following policies: ● Information Policy ● Information Security Policy ● Information Security Incident Reporting Policy ● Acceptable Use Policy ● Records Management Policy ● Archive Policy ● Surveillance Policy ● Biometric These policies set out the processes in place to ensure that the purposes and duration for which special category data are held are not exceeded and the security mechanisms and procedures that are in place to keep this information secure. Administrative procedures for ensuring personal data is recorded accurately and kept up to date are also documented. These policies are regularly in line with the Trust's policy review schedule to ensure the processes, procedures and measures remain appropriate and effective.
Information Asset Register	Lawfulness, fairness and transparency Purpose limitation Security	Maintenance of this document fulfils the Trust's legal obligation under Article 30 of the General Data Protection Regulation to keep a record of its processing activities. Information assets which contain special category data have been identified and Article 6, Article 9 and Schedule 1 conditions (where applicable) have been identified for each asset. Retention periods for each asset, based on the Trust's retention schedule, have also been identified, along with the technical and organisational security measures that are in place to protect each asset. This document is reviewed regularly and updated where there have been changes to the trust's data processing.

Data Protection Impact Assessments (DPIAs)	Accountability Lawfulness fairness and transparency Purpose limitation Data minimisation Accuracy	The Trust conducts Data Protection Impact Assessments where it is undertaking new, high risk processing, or making significant changes to existing data processing. The purpose of the DPIA is to consider and document the risks associated with a project prior to its implementation, ensuring data protection is embedded by design and default. All of the data protection principles are assessed to identify specific risks. These risks are then evaluated and solutions to mitigate or eliminate these risks are considered. Where a less privacy-intrusive alternative is available, or the project can go ahead without the use of special category data, the trust will opt to do this. All DPIAs are signed by the school's Senior Information Risk Owner and Data Protection Officer.
Mandatory data protection training	Accountability Security	All staff undertake mandatory data protection training every 2 years as a minimum, with annual refresher training if resources allow. (Training should be undertaken for all new staff.) Staff members who have particular responsibility for managing the risks to personal data, such as the Senior Information Risk Owner, Specific Point of Contact and Information Asset Owners, undertake additional specialist training where applicable. Where new processes are introduced as a result of additions to or changes to processing, additional training will be provided to staff members involved with the project. The requirement for this will be identified as part of Data Protection Impact Assessments.
Retention schedule and destruction log	Purpose limitation Data minimisation	The Trust does not retain special categories of data for any longer than it is necessary to do so in order to fulfil our specific purposes. The Trust has a retention schedule in place which is based on guidance issued by the Information and Records Management Society (IRMS). Where there is no legislative or best practice guidance in place, the Senior Information Risk Owner will decide how long the information should be retained based on the necessity to keep the information for a legitimate purpose or purposes. The Headteacher in each school has responsibility for ensuring records retention periods are adhered to. The Trust also maintains a destruction log, which documents what information has been destroyed, the date it was destroyed and why it has been destroyed.

Technical and organisational security measures and procedures. Recording and reporting personal data breaches where necessary	Security Accountability Accuracy	The Trust employs the following technical and organisational security measures where appropriate to protect the personal and special category data that the Trust processes: ● Password protection of electronic devices and systems ● Encryption of portable devices ● Encryption of emails for the sending of sensitive data ● Recorded delivery of sensitive paper documents ● Secure, fireproof storage of paper records using a key/ PIN management system ● Audit trails on electronic systems ● Regular backups that can be restored in the event of an emergency ● Access/ permission controls ● Secure destruction of paper records ● Information governance policies (detailed above) ● Physical building security measures (locked doors, visitor sign in procedure, alarm system, CCTV etc.) ● Cyber security risk prevention measures (firewalls and anti-virus software, phishing email awareness, download restrictions etc.) A full description of security measures employed by the Trust can be found in the Trust's Information Security Policy referenced above. In the event that these measures should fail and a personal data breach occurs, the incident will be recorded in a log, investigated and reported to the trust's Data Protection Officer where necessary. Severe incidents are reported to the Information Commissioner's Office. This process is documented in greater detail in the Information Security Incident Reporting Policy referred to above.
Written contracts with data processors	Accountability Security	Where the Trust shares personal data with a data processor, a written contract is obtained. All existing contracts are checked to ensure that all mandatory data protection clauses are present and all new contracts are assessed prior to forming an agreement with the processor.
Compliance with data rights requests	Lawfulness, fairness and transparency Accountability	The Trust maintains a log of all data rights requests and has appropriate processes set out in the Trust's policies for handling such requests.

	Accuracy	
Data Protection Officer	Accountability	The Trust has appointed a Data Protection Officer to oversee the Trust's compliance with the data protection principles.

Retention of special category and criminal convictions data

The retention periods of special category and criminal convictions data are set out in the Trust's retention schedule, which is based on the Information and Records Management Society (IRMS) Toolkit for Schools. Retention periods of specific information assets are identified in the Trust's information asset register and the Trust has adopted a Records Management Policy, as referred to above.