SUCCESS FOR ALL
EDUCATIONAL TRUST

DATA PROTECTION POLICY

January 2026

Success for all Educational Trust
DATA PROTECTION POLICY

Document Management Information	
Applicable to:	All Trustees, Members, Governors, Trust Staff
Dissemination:	This policy will be made available on the Trust's website.
Review frequency:	This policy will be reviewed annually
Policy Author:	Sarah Garman, Data & MIS Officer
Approval by:	FAR Committee
Approval Date:	26/02/2026
Next Review Due:	January 2027

Revision History

Document version	Description of revision	By whom	Date Approved
v1.1	ICO Registration Details added, Criminal Record Data Processing updated	S Garman	26/02/2026
v1.2	Updates to data withdrawal, data requests procedures, key staff changes	J Adams	25/09/2026

Introduction

The UK General Data Protection Regulation (UK GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the

rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The Trust will protect and maintain a balance between data protection rights in accordance with the UK GDPR. This policy sets out how we handle the personal data of our pupils, parents, suppliers, employees, workers and other third parties.

This policy complements the individual's terms and conditions of employment with the Trust and should be read in conjunction with relevant contractual obligations regarding data protection. This policy will be reviewed and updated at least annually, or more frequently if required by changes in legislation or ICO guidance. All revisions will be documented and communicated to relevant staff members.

All staff members will receive mandatory data protection training, covering the key principles of data protection, data subject rights, and the Trust's data protection policies and procedures. Refresher training will be provided periodically to ensure ongoing awareness and compliance. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the Trust's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

The School is registered with the Information Commissioners Office (ICO) as required (Registration No. ZB205602).

Section 1 – Definitions

Personal data

Personal data is any information relating to an individual who can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access, including online identifiers (such as IP addresses and cookies) and offline identifiers (such as physical addresses and identification numbers). This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

Special Category Data

Previously termed “Sensitive Personal Data” " special Category Data is similar by definition and refers to data concerning an individual Data Subject’s racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

Data Subject

An individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees.

Data Controller

'SFAET LTD' is the Data Controller for the purposes of the UK GDPR and is responsible for the processing of personal data under this policy.

Processing

Processing data involves any activity that involves the use of personal data. This includes but is not limited to obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

Automated Processing

Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular, to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

An example of automated processing includes profiling and automated decision-making. Automatic decision-making is when a decision is made which is based solely on automated processing (without human intervention) which produces legal effects or significantly affects an individual. Automated decision-making, including profiling, will only be used in exceptional circumstances where permitted by law and where appropriate safeguards are in place. Such safeguards may include human review of the decision, the right to contest the decision, and ensuring data accuracy.

Data Protection Impact Assessment (DPIA)

DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

Criminal Records Information

This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

Section 2 – When can the Trust Process Personal Data?

Data Protection Principles

The Trust is responsible for and adheres to the principles relating to the processing of personal data as set out in the UK GDPR. The principles the Trust must adhere to are set out below.

Principle 1: Personal data must be processed lawfully, fairly and in a transparent manner

The Trust only collects, processes and shares personal data fairly and lawfully and for specified purposes. The Trust must have a specified purpose for processing personal data and special category data as set out in the UK GDPR.

Before the processing starts for the first time, we will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. We will then regularly review those purposes whilst processing continues to satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e., that there is no other reasonable way to achieve that purpose).

Personal Data

The Trust may only process a data subject's personal data if one of the following fair processing conditions are met: -

- The data subject has given their consent;
- The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- To perform a task in the public interest or in order to carry out official functions as authorised by law;
- For the purposes of the Trust's legitimate interests where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject.

Special Category Data

The Trust may only process special category data if they are entitled to process personal data (using one of the fair processing conditions above) AND one of the following conditions are met: -

- The data subject has given their explicit consent;
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the Trust in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- Where the data has been made public by the data subject;
- To perform a task in the substantial public interest or in order to carry out official functions as authorised by law;
- Where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
- Where it is necessary for reasons of public interest in the area of public health;
- Processing is required for archival, statistical or research purposes.

The Trust identifies and documents the legal grounds being relied upon for each processing activity.

Criminal Record Data

Where criminal records data is processed, a lawful condition for processing that data is also identified and documented.

Consent

Where the Trust relies on consent as a fair condition for processing (as set out above), it will adhere to the requirements set out in the UK GDPR.

Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent is needed in cases of processing special category data and requires a very clear and specific statement to be relied upon (i.e. more than just mere action is required).

A data subject will have consented to processing of their non-special category personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

In cases of processing special category data and explicit consent, the Trust will normally seek another legal basis to process that data. However, if explicit consent is required, the data subject will be provided with full information in order to provide explicit consent.

The Trust will keep records of consents obtained in order to demonstrate compliance with consent requirements under the UK GDPR.

Principle 2: Personal data must be collected only for specified, explicit and legitimate purposes

Personal data will not be processed in any matter that is incompatible with legitimate purposes.

The Trust will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the data subject of the new purpose (and they have consented where necessary).

Principle 3: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed

The Trust will only process personal data when our obligations and duties require us to. We will not collect excessive data and ensure any personal data collected is adequate and relevant for the intended purposes.

When personal data is no longer needed for specified purposes, the Trust shall delete or anonymise the data. Please see Trust's Data Retention Policy for further guidance.

Principle 4: Personal data must be accurate and, where necessary, kept up to date

The Trust will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

Data subjects also have an obligation to ensure that their data is accurate, complete, up-to-date and relevant. Data subjects have the right to request rectification of incomplete or inaccurate data held by the Trust.

Principle 5: Personal data must not be kept in a form which permits the identification of data subjects for longer than is necessary for the purposes for which the data is processed

Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The Trust will ensure that they adhere to legal timeframes for retaining data.

We will take reasonable steps to destroy or erase from our systems all personal data that we no longer require. We will also ensure that data subjects are informed of the period for which data is stored and how that period is determined in our privacy notices.

Please refer to the Trust's Retention Policy for details on how the Trust retains and removes data.

Principle 6: Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage

To ensure the protection of all data being processed, the Trust will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as: -

- Encryption;
- Pseudonymisation (this is where the Trust replaces information that directly or indirectly identifies an individual with one or more artificial

identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure);

- Ensuring authorised access on both hard copy and electronic files (i.e. that only people who have a need to know the personal data are authorised to access it);
- Adhering to confidentiality principles;
- Ensuring personal data is accurate and suitable for the process for which it is processed.

The Trust follows procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data.

The Trust will only transfer personal data to third-party service providers who have entered into a written data processing agreement that meets the requirements of the UK GDPR. This agreement will specify the purpose of processing, data security standards, and data subject rights.

Sharing Personal Data

The Trust will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. The following points will be considered:

- Whether the third party has a need to know the information for the purposes of providing the contracted services;
- Whether sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained;
- Whether the third party has agreed to comply with the required data security standards, policies and procedures and implemented adequate security measures;
- Whether the transfer complies with any applicable cross-border transfer restrictions; and
- Whether a fully executed written contract that contains UK GDPR approved third-party clauses has been obtained.

There may be circumstances where the Trust is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities for example, the Local Authority, Ofsted or the Department of Health. These authorities are up to date with data protection laws and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of the Trust shall be clearly defined within written notifications including details and the basis for sharing the data.

Transfer of Data Outside the European Economic Area (EEA)

The UK GDPR restricts data transfers to countries outside the EEA to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined.

The Trust will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the UK GDPR. All staff must follow the Trust's guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

Transfer of Data Outside the UK

The Trust may transfer personal data to countries, territories, or organisations that have been designated by the UK government as providing an adequate level of protection for personal data. The current list of these countries/territories/organisations can be found on the ICO website. If the recipient country/territory/organisation has not been designated as providing adequate protection, the Trust will implement appropriate safeguards for international data transfers. These safeguards may include Standard Contractual Clauses, Binding Corporate Rules, or approved codes of conduct. The specific safeguards used will be documented and assessed for suitability.

Section 3 – Data Subject's Rights and Requests

Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data.
The rights data subjects have in relation to how the Trust handle their personal data are set out below: -

(a) (Where consent is relied upon as a condition of processing) To withdraw consent to processing at any time;

(b) Receive certain information about the Trust's processing activities;

(c) Request access to their personal data that we hold (see "Subject Access Requests" in Appendix 1);

(d) Prevent our use of their personal data for marketing purposes;

(e) Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed to rectify inaccurate data or to complete incomplete data;

(f) Restrict processing in specific circumstances;

(g) Challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) Request a copy of an agreement under which personal data is transferred outside of the EEA;

(i) Object to decisions based solely on automated processing;

(j) Prevent processing that is likely to cause damage or distress to the data subject or anyone else;

(k) Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

(l) Make a complaint to the supervisory authority; and

(m) In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

If any request is made to exercise the rights above, it is a requirement for the relevant staff member within the Trust to verify the identity of the individual making the request.

Direct Marketing

The Trust is subject to certain rules and privacy laws when marketing. For example, a data subject's prior consent will be required for electronic direct marketing (for example, by email, text or automated calls).

The Trust will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The Trust will promptly respond to any individual objection to direct marketing.

Employee Obligations

Employees who have access to personal data in the course of their employment are responsible for adhering to this policy and maintaining confidentiality. This includes ensuring the security of personal data, limiting access to authorised individuals, and reporting any data protection concerns to the Data Protection Officer. If so, the Trust expects those employees to help meet the Trust's data protection obligations to those individuals. Specifically, you must: -

- Only access the personal data that you have authority to access, and only for authorised purposes;
- Only allow others to access personal data if they have appropriate authorisation;
- Keep personal data secure (for example, by complying with rules on access to school premises, computer access, password protection and secure file storage and destruction;
- Not remove personal data or devices containing personal data from the Trust premises unless appropriate security measures are in place (such as pseudonymisation, encryption, password protection) to secure the information;
- Personal data should be stored securely on designated Trust systems and in accordance with the Trust's data security policies. Storage of personal data on local drives or personal devices is generally prohibited unless explicitly authorised and appropriate security measures are in place.

Section 4 - Accountability

The Trust will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. We are responsible and accountable with the UK GDPR principles.

The Trust has taken the following steps to ensure and document UK GDPR compliance:-

Data Protection Officer (DPO)

Please find below details of the Trust's Data Protection Officer: -

Data Protection Officer: Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB
Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 (option 1, then option 1 again)

The DPO is responsible for overseeing this Data Protection Policy and developing data-related policies and guidelines.

Should you have any questions about the UK GDPR, the operation of this policy or, if you have any concerns that this policy is not being, or has not been, followed, please contact Mrs S Garman (sgarman@sfaet.co.uk) in the first instance. Should the matter remain unresolved or require further escalation, please contact the school's DPO (dataservices@judicium.co.uk).

In particular, you must always contact the DPO in the following circumstances: -

(a) If you are unsure of the lawful basis being relied on by the Trust to process personal data;

(b) If you need to rely on consent as a fair reason for processing (please see below the section on consent for further details);

(c) If you need to draft privacy notices or fair processing notices;

(d) If you are unsure about the retention periods for the personal data being processed but would refer you to the Trust's Data Retention Policy in the first instance;

(e) If you are unsure about what security measures need to be put in place to protect personal data;

(f) If there has been a personal data breach and would refer you to the procedure set out in the Trust's Data Breach Policy;

(g) If you are unsure on what basis to transfer personal data outside the EEA;

(h) If you need any assistance dealing with any rights invoked by a data subject;

(i) Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for;

(j) If you plan to undertake any activities involving automated processing or automated decision-making;

(k) If you need help complying with applicable law when carrying out direct marketing activities;

(l) If you need help with any contracts or other areas in relation to sharing personal data with third parties.

Personal Data Breaches

The UK GDPR requires the Trust to notify any applicable personal data breach to the Information Commissioner's Office (ICO).

We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person designated as the key point of contact for personal data breaches who is the Trust's Director of Operation.

Transparency and Privacy Notices

The Trust will provide data subjects with clear and concise privacy notices that explain how their personal data is collected, used, and protected. These notices will include information on the purpose of processing, data retention periods, data subject rights, and contact details for the Data Protection Officer. This information will be provided through the Trust's privacy notices which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. The Trust's privacy notices are tailored to suit the data subject and set out information about how the Trust uses their data.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the UK GDPR. This includes the identity of the Data Protection Officer, the Trust's contact details, and how and why we will use, process, disclose, protect and retain personal data. This information will be provided within our privacy notices.

When personal data is collected indirectly (for example, from a third party or a publicly available source), where appropriate, we will provide the data subject with the above information as soon as possible after receiving the data. The Trust will also confirm whether that third party has collected and processed data in accordance with the UK GDPR.

Notifications shall be in accordance with ICO guidance and where relevant, be written in a form understandable by those defined as "children" under the UK GDPR.

Privacy by Design

The Trust embeds privacy by design principles into all new projects and processes involving the processing of personal data. This includes conducting Data Protection Impact Assessments (DPIAs), minimising the collection of personal data, and implementing appropriate technical and organisational security measures from the outset.

Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the Trust takes into account the nature and purposes of the processing, any cost of implementation and any risks to the rights and freedoms of data subjects when implementing data processes.

Data Protection Impact Assessments (DPIAs)

To achieve a privacy-by-design approach, the Trust conducts DPIAs for any new technologies or programmes being used by the Trust which could affect the processing of personal data. In any event, the Trust carries out DPIAs when required by the UK GDPR in the following circumstances: -

- For the use of new technologies (programs, systems or processes) or changing technologies;
- For the use of automated processing;
- For large-scale processing of special category data; and
- For large-scale, systematic monitoring of a publicly accessible area (through the use of CCTV).

Our DPIAs contain: -

- A description of the processing, its purposes and any legitimate interests used;
- An assessment of the necessity and proportionality of the processing in relation to its purpose;
- An assessment of the risk to individuals; and
- The risk mitigation measures in place and demonstration of compliance.

Record Keeping

The Trust maintains a record of all data processing activities, including a data processing inventory that documents the purpose, legal basis, data categories, and data subject types for each processing activity. This inventory is regularly reviewed and updated to ensure accuracy and compliance. These records include: -

- The name and contact details of the Trust;
- The name and contact details of the Data Protection Officer;
- Descriptions of the types of personal data used;
- Description of the data subjects;
- Details of the Trust's processing activities and purposes;
- Details of any third-party recipients of the personal data;
- Where personal data is stored;
- Retention periods; and
- Security measures in place.

Training

All staff members who handle personal data will receive mandatory data protection training upon induction and at least every two years thereafter. The training will cover

relevant legislation, data protection principles, data subject rights, and the Trust's data protection policies and procedures.

Audit

The Trust conducts regular data protection audits and reviews to assess compliance with data protection legislation and this policy. The Data Protection Officer will conduct these audits at least annually and will cover areas such as data security, data retention, and data subject rights. Data protection audits will assess the effectiveness of the Trust's data protection measures and identify any areas for improvement. The audits will cover areas such as data security, data retention, data subject rights, and compliance with data protection legislation and this policy.

Related Policies

Staff should refer to the following policies that are related to this Data Protection Policy: -

Data Retention Policy

Data Breach Policy

Staff Privacy Notice

Student and Staff Privacy Notice

Monitoring

We will monitor the effectiveness of this and all our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the Trust.

Review

This policy will be reviewed and amended as necessary.

Policy date: January 2026

Next review date: January 2027

Reviewed by: Sarah Garman, Trust Data & MIS Officer

Signature of CEO:……
Date:……

Signature of Chair of Trustees:……..
Date:……..

Appendix 1 – Subject Access Requests

Under Data Protection Law, data subjects have a general right to find out whether the Trust holds or processes personal data about them, to access that data, and to be given supplementary information. This is known as the right of access or the right to make a data subject access request (SAR). The purpose of the right is to enable the individual to be aware of and verify the lawfulness of the processing of personal data that the Trust is undertaking.

This appendix provides guidance for staff members on how data subject access requests should be handled and for all individuals on how to make a SAR.

Failure to follow the right of access under UK GDPR puts both staff and the Trust at potentially significant risk and so the Trust takes compliance with this policy very seriously.

A data subject has the right to be informed by the Trust of the following: -

(a) Confirmation that their data is being processed;
(b) Access to their personal data;
(c) A description of the information that is being processed;
(d) The purpose for which the information is being processed;
(e) The recipients/class of recipients to whom that information is or may be disclosed;
(f) Details of the Trust's sources of information obtained;
(g) In relation to any personal data processed for the purposes of evaluating matters in relation to the data subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct; and
(h) Other supplementary information.

How to Recognise a Subject Access Request

A data subject access request is a request from an individual (or from someone acting with the authority of an individual, e.g., a solicitor or a parent making a request in relation to information relating to their child):

- for confirmation as to whether the Trust process personal data about him or her and, if so
- for access to that personal data
- and/or certain other supplementary information

A valid SAR can be both in writing (by letter, email, WhatsApp text) or verbally (e.g., during a telephone conversation). The request may refer to the UK GDPR and/or to

'data protection' and/or to 'personal data' but does not need to do so to be a valid request. For example, a letter which states 'please provide me with a copy of information that the Trust holds about me' would constitute a data subject access request and should be treated as such.

A data subject is generally only entitled to access their own personal data and not information relating to other people.

How to Make a Data Subject Access Request

Whilst there is no requirement to do so, we encourage any individuals who wish to make such a request to make the request in writing, detailing exactly the personal data being requested. The Trust operates a dedicated GDPR hub, on their website, which allows the Trust to easily recognise that you wish to make a data subject access request and the nature of your request. If the request is unclear/vague we may be required to clarify the scope of the request which may in turn delay the start of the time period for dealing with the request.

What to do When You Receive a Data Subject Access Request

All data subject access requests should be immediately directed to the school's delegated member of staff for handling data requests, who will report these to the Head of IT and Data and Judicium as DPO to assist with the request and what is required. There are limited timescales within which the Trust must respond to a request and any delay could result in failing to meet those timescales, which could lead to enforcement action by the Information Commissioner's Office (ICO) and/or legal action by the affected individual.

Acknowledging the Request

When receiving a SAR the Trust shall acknowledge the request as soon as possible and inform the requester about the statutory deadline (of one calendar month) to respond to the request.

In addition to acknowledging the request, the Trust may ask for:

- proof of ID (if needed);
- further clarification about the requested information;
- if it is not clear where the information shall be sent, the Trust must clarify what address/email address to use when sending the requested information; and/or
- consent (if requesting third party data).

The Trust should work with their DPO to create the acknowledgment.

Verifying the Identity of a Requester or Requesting Clarification of the Request

Before responding to a SAR, the Trust will take reasonable steps to verify the identity of the person making the request. For current employees, this will usually be straightforward. The Trust is entitled to request additional information from a requester to verify whether the requester is in fact who they say they are. Where the Trust has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of a passport, driving licence, a recent utility bill with current address, birth/marriage certificate, credit card or a mortgage statement.

If an individual is requesting a large amount of data the Trust may ask the requester for more information for the purpose of clarifying the request. The requester shall never be asked why the request has been made. The Trust shall let the requestor know as soon as possible where more information is needed before responding to the request.

In both cases, the response period begins when additional information has been received. If the Trust does not receive this information, they will be unable to follow the request.

Requests Made by Third Parties or on Behalf of Children

The Trust needs to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney. The Trust may also require proof of identity in certain circumstances.

If the Trust is in any doubt or has any concerns as to providing the personal data of the data subject to the third party, then it should provide the information requested directly to the data subject. It is then a matter for the data subject to decide whether to share this information with any third party.

When requests are made on behalf of children, it is important to note that even if a child is too young to understand the implications of subject access rights, it is still the right of the child, rather than of anyone else such as a parent or guardian, to have access to the child's personal data. Before responding to a SAR for information held about a child, the Trust should consider whether the child is mature enough to understand their rights. If the Trust is confident that the child can understand their rights, then the Trust should usually respond directly to the child or seek their consent before releasing their information.

It shall be assessed if 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. When considering borderline cases, it should be taken into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

Generally, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 12 years of age or older, then provided that the Trust is confident that they understand their rights and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the Trust will require the written authorisation of the child before responding to the requester or provide the personal data directly to the child.

The Trust may also refuse to provide information to parents if there are consequences of allowing access to the child's information – for example, if it is likely to cause detriment to the child.

Fee For Responding to a SAR

The Trust will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive a fee to cover administrative costs may be requested. If a request is considered to be manifestly unfounded or unreasonable the Trust will inform the requester why this is considered to be the case and that the Trust will charge a fee for complying with the request.

A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged taking into account the administrative costs of providing the information.

If a fee is requested, the response period begins when the fee has been received.

Time Period for Responding to a SAR

The Trust has one calendar month to respond to a SAR. This will run from the day that the request was received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received.

The circumstances where the Trust is in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity and in the case of a third party requester, the written authorisation of the data subject has been received.

The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

Where a request is considered to be sufficiently complex as to require an extension of the period for response, the Trust will need to notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

School Closure Periods

The school may not be able to respond to requests received during or just before school closure periods within the one calendar month response period. This is because the School will be closed and no one will be on site to follow the request.. As a result, it is unlikely that your request will be able to be processed during this time. We may not be able to acknowledge your request during this time (i.e., until a time when we receive the request). However, if we can acknowledge the request, we may still not be able to deal with it until the schools re-opens. The Trust will endeavour to comply with requests as soon as possible and will keep in communication with you as far as possible. If your request is urgent, please provide your request during term times and not during/close to closure periods.

Information to be Provided in Response to a Request

The individual is entitled to receive access to the personal data we process about him or her and the following information:

- the purpose for which we process the data;
- the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular where those recipients are in third countries or international organisations;
- where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period;

- the fact that the individual has the right:
  - to request that the Company rectifies, erases or restricts the processing of his personal data; or
  - to object to its processing;
  - to lodge a complaint with the ICO;
  - where the personal data has not been collected from the individual, any information available regarding the source of the data;
  - any automated decision we have taken about him or her together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for him or her.

The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. The response shall be given in writing if the SAR was made in writing in a commonly used electronic format.

The information that the Trust is required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as the Trust has one month in which to respond the Trust is allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the SAR.

Therefore, the Trust is allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. The Trust is not allowed to amend or delete data to avoid supplying the data.

How to Locate Information

The personal data the Trust needs to provide in response to a data subject access request may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

Depending on the type of information requested, the Trust may need to search all or some of the following:

- electronic systems, e.g., databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV;
- manual filing systems in which personal data is accessible according to specific criteria, e.g., chronologically ordered sets of manual records containing personal data;
- data systems held externally by our data processors;

- occupational health records;
- pensions data;
- share scheme information;
- insurance benefit information.

The Trust should search these systems using the individual's name, employee number or other personal identifier as a search determinant.

Protection of Third Parties - Exemptions to the Right of Subject Access

There are circumstances where information can be withheld pursuant to a SAR. These specific exemptions and requests should be considered on a case by case basis.

The Trust will consider whether it is possible to redact information so that this does not identify those third parties. If their data cannot be redacted (for example, after redaction it is still obvious who the data relates to) then the Trust do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information unless:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information without the individual's consent, all of the relevant circumstances will be taken into account, including:

- the type of information that they would disclose;
- any duty of confidentiality they owe to the other individual;
- any steps taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to the Trust disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the Trust must decide whether to disclose the information anyway. If there are any concerns in this regard then the DPO should be consulted.

Other Exemptions to the Right of Subject Access

In certain circumstances, the Trust may be exempt from providing some or all requested personal data. These exemptions are described below and should only be applied on a case-by-case basis after careful consideration of all the facts.

Crime detection and prevention: The Trust does not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

Confidential references: The Trust does not have to disclose any confidential references given to, or received from, third parties for the purpose of actual or prospective:

- education, training or employment of the individual;
- appointment of the individual to any office; or
- provision by the individual of any service

Legal professional privilege: The Trust does not have to disclose any personal data which is subject to legal professional privilege.

Management forecasting: The Trust does not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.

Negotiations: The Trust does not have to disclose any personal data consisting of records of intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

Refusing to Respond to a Request

The Trust can refuse to comply with a request if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If a request is found to be manifestly unfounded or excessive the Trust can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

In either case, the Trust must justify the decision and inform the requester about the decision.

The reasonable fee should be based on the administrative costs of complying with the request. If deciding to charge a fee the Trust should contact the individual promptly and inform them. The Trust does not need to comply with the request until the fee has been received.

Record Keeping

Sarah Garman, Trust MIS and Data Officer shall keep a record of all subject access requests. The record shall include the date the SAR was received, the name of the requester, what data the Trust sent to the requester and the date of the response.

Appendix 2 - Biometrics Policy

What is biometric data?

Biometric data means personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.
All biometric data is considered to be special category data under the General Data Protection Regulation (GDPR). This means the data is more sensitive and requires more protection and this type of data could pose more significant risks to a person's fundamental rights and freedoms.
This policy complies with The Protection of Freedoms Act 2012 (sections 26 to 28), the Data Protection Act 2018 and the GDPR.

What is an automated biometric recognition system?
An automated biometric recognition system uses technology which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically). Information from the individual is automatically compared with biometric information stored in the system to see if there is a match to recognise or identify the individual.

The legal requirements under GDPR

'Processing' of biometric information includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including (but not limited to) disclosing it, deleting it, organising it or altering it.

As biometric data is special category data to lawfully process this data, each school in the Trust must have a legal basis for processing personal data and a separate condition for processing special category data. When processing biometric data, each school relies on explicit consent (which satisfies the fair processing conditions for personal data and special category data).
The schools process biometric data for the specific purposes of facilitating cashless payments in the canteen and managing access control to lunch facilities.

Consent and withdrawal of consent

The schools will not process biometric information without the relevant consent.

Consent for students

When obtaining consent for students, both parents will be notified that the school intends to use and process their child's biometric information. The school only requires written consent from one parent (in accordance with the Protection of Freedoms Act 2012), provided no parent objects to the processing.

If a parent objects to the processing, then the school will not be permitted to use that child's biometric data and alternatives will be provided.

The child may also object to the processing of their biometric data. If a child objects, the school will not process or continue to process their biometric data, irrespective of whether consent has been provided by the parent(s).

Where there is an objection to the processing of biometric data, the school will provide reasonable alternatives, such as the use of a PIN code, contactless card, or manual identification, to ensure the child can access the same facilities.

Students and parents can withdraw their consent to the use of biometric data at any time. Consent can be withdrawn by contacting the school office.

Students who wish for the school to stop using their biometric data do not have to put this in writing but should inform their teacher(s) or a member of school staff so that the school can address this for them.

The consent will last for the time period that your child attends the school (unless it is withdrawn).

Consent for staff (if biometric data is used)

The Trust will seek consent from staff before processing their biometric data. Staff can withdraw their consent at any time by writing to their schools designated member of staff for handling data requests, usually the Headteachers PA, Human Resources team, or by contacting their Headteacher.

The consent will last for the period the employee remains employed by the Trust (unless it is withdrawn).

Retention of Biometric Data

Biometric data will be retained for the duration of a student's enrolment at the school or a staff member's employment with the Trust unless consent is withdrawn earlier. Upon withdrawal of consent or the end of the enrolment/employment, biometric data will be securely deleted within 72 hours.

Once a student or staff member leaves, the biometric data will be deleted from the school's system no later than 72 hours. At the point that consent is withdrawn, the schools will take steps to delete their biometric data from the system no later than 72 hours.

Storage of Biometric Data

Biometric data will be stored securely on encrypted systems with restricted access controls. The Trust will implement appropriate technical and organisational security measures to protect biometric data from unauthorised access, use, disclosure, alteration, or destruction. These measures will include regular security assessments, staff training, and data breach response procedures.

Schools across the Trust have very limited amounts of biometric data and have a legitimate interest in collecting students biometric data, for cashless catering purposes in the form of student's finger prints (usually their thumb print), to link to their payment accounts for purchasing goods from school canteens.