DMAT

Aspiration | Excellence | Transformation

Data Protection Policy (including SAR appendix) 2026 -2027

Compiled/ Reviewed and Updated	**Author:** Dave Hutchinson	**Date:** May 2026
Approval By: CEO/ Executive Team Pauline Montalto	**Approval Date:** 08 May 2026	**Review Date:** May 2027

Contents

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 does not form part of any individual's terms and conditions of employment with the Trust and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy to remain compliant with legal obligations.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Staff is defined by employees, governors, trustees, and volunteers. A 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 dismissal depending on the seriousness of the breach.

The Term 'Trust' includes the schools and organisations within the Trust.

Section 1 - Definitions

Personal Data	Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymises 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 and Data Relating to Criminal Convictions and Offences	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 opinions, religious or philosophical beliefs, trade union membership, physical and mental health, sexuality and biometric or genetic data. Personal data relating to criminal offences and convictions is included here for the purposes of this policy. This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.
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	The organisation storing and controlling such information (i.e., the Trust) is referred to as the data controller.
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 is prohibited except in exceptional circumstances.
Data Protection Impact Assessment (DPIA)	DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.
Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Pseudonymised	The process by which personal data is processed in such a way that that it cannot be used to identify an individual without the use of

	additional data, which is kept separately and subject to technical and organisational measures to ensure that the personal data cannot be attributed to an identifiable individual.

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 collect, process, and share 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 in order 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 were 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 welfare 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;
- 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, welfare benefits law, or social welfare law. This includes the processing of special category personal data, as defined under the UK GDPR, where required for these purposes. This may include, but is not limited to, managing sickness absence, addressing disability, and making reasonable adjustments, arranging private health care insurance, and providing contractual sick pay.

- To protect the data subject's vital interests;
- The processing is necessary for the establishment, exercise, or defence of legal claims or whenever courts are acting in their judicial capacity
- 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 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;
- The processing is necessary for archiving, statistical or research purposes.

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

Criminal Record Data

Criminal records data is processed, also identify a lawful condition for processing that data and document it.

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 manner that is incompatible with the legitimate purposes specified.

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 will 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 refer to the 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 to incomplete or inaccurate data held by the Trust.

Principle 5: Personal data must not be kept in a form which permits 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 further details about how the Trust retains and removes data.

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

In order 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
- 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 follow 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 agree to comply with the required policies and procedures and agree to put adequate measures in place.

Sharing Personal Data

The Trust will generally not share personal data with third parties unless a DPIA has been carried out. The following points will be considered:

- Whether the third party has a need to know the information for the purposes of providing the contracted service;
- 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

- 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 law 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)

Where adequacy does not apply, the Trust will use appropriate safeguards under Article 46 UK GDPR, including the ICO International Data Transfer Agreement (IDTA) or the UK Addendum to the EU Standard Contractual Clauses, and will complete a Transfer Risk Assessment (TRA) to document that protections for data subjects are not undermined.

The UK GDPR restricts data transfers to countries outside the EEA in order 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 comply with 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

UK–US Data Bridge: Where transfers are made to organisations in the United States that are certified under the UK Extension to the EU–US Data Privacy Framework (the UK–US Data Bridge), those transfers may take place without the need for the IDTA/Addendum. The Trust will verify recipient certification status (including HR data coverage where relevant) and record this in our RoPA.

The Trust may transfer personal information outside the UK and/or to international organisations on the basis that the country, territory, or organisation is designated as having an adequate level of protection. Alternatively, the organisation receiving the information has provided adequate safeguards by way of binding corporate rules, Standard Contractual Clauses, or compliance with an approved code of conduct.

Section 3 – Data subjects' 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 handles their personal data are set out below:

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

(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 or 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, which is the Information Commissioner in England and Wales https://ico.org.uk/global/contact-us

(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 may have access to the personal data of other members of staff, suppliers, parents, or pupils of the Trust in the course of their employment or engagement. 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 Trust 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

Section 4 – Accountability

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

The Trust has taken the following steps to ensure and document UK GDPR compliance: appointed an external and internal data protection officer

External Data Protection Officer (DPO)

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

Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 option 1 then option 1 again

Internal Data Protection Officer (DPO)

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

Please email dpo@dmat.education with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this policy is not being or has not been followed. 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 detail)

(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. Please refer 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. Please refer 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

In line with UK GDPR and ICO guidance, notifiable personal data breaches must be reported to the ICO without undue delay and, where feasible, within 72 hours of becoming aware of the breach. If the report is made after 72 hours, reasons for the delay must accompany the notification. Individuals must also be informed without undue delay where there is a high risk to their rights and freedoms.

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. Please refer to our Data Breach policy.

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: dpo@dmat.education

Transparency and Privacy Notices

Children's Code: For any online services likely to be accessed by children, the Trust will conform with the ICO's Age Appropriate Design Code (Children's Code), including high privacy by default, data

minimisation, geolocation off by default, profiling off by default unless in the best interests of the child, and age-appropriate transparency.

The Trust will provide detailed, specific information to data subjects. 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 contact details, 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 adopts a privacy by design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.

Privacy by design is an approach that promotes privacy and data protection compliance from the start by undertaking a Data Protection Impact Assessment (DPIA). 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 rights and freedoms of data subjects when implementing data processes.

Data Protection Impact Assessments (DPIAs)

The Trust conducts DPIAs for any new high-risk technologies or programmes being used by the Trust which could affect the processing of personal data. 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
- 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
- Details of what types of data are shared
- Steps taken by the third party and the Trust in order to protect data
- An assessment of the necessity and proportionality of the processing in relation to its purpose
- An assessment of the risk to individuals
- The risk mitigation measures in place and demonstration of compliance.

Record Keeping

The Trust is required to keep full and accurate records of our data processing activities. These records include:

- The name and contact details of the Trust
- The name and contact details of the Data Protection Office;
- 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
- Security measures in place

Training

The Trust will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws. The Trust will carry out adequate training with all staff and staff will complete the TES Develop GDPR module upon induction and then annually and will also have an annual face to face GDPR update. Training will include annual INSET day updates on previous years GDPR activity.

Audit

The Trust regularly tests our data systems and processes in order to assess compliance. These are done through data audits which take place regularly in order to review use of personal data.

Related Policies

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

DMAT CCTV Policy

DMAT Data Breach Policy

DMAT Data Retention Policy

DMAT Freedom of Information Policy

DMAT Privacy Notice Governors and Volunteers

DMAT Privacy Notice Job Applicants

DMAT Privacy Notice Pupils and Parents

DMAT Privacy Notice Staff

These policies and notices are also designed to protect personal data and can be found on the Trust website and school websites.

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.

Appendix 1 – Subject Access Requests

Under Data Protection Law, data subjects have a general right to find out whether the Trust hold or process 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 are undertaking. It is designed to assist individuals in understanding how and why we are using their data and to check that we are doing so lawfully. The main provisions are to be found in Articles 12 and 15 of the UK GDPR and Section 45 of the Data Protection Act 2018.

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 comply with 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 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
(g) Other supplementary information

Dealing with a SAR is time critical and must be prioritised. Other than in exceptional cases, the Trust has one month in which to respond to a SAR and even if an extension of the time limit is permitted, the individual must still be informed within that month of the fact that the request will take longer to process and the reasons for the delay. Failure to deal with a SAR within that period could lead to the possibility of being fined by the ICO.

All staff must be aware of the potential for receiving a SAR and the importance of dealing with such as request as a matter of urgency.

Anyone within the Trust may receive a SAR. It does not need to be made to a nominated person or even to a person responsible for dealing with either the data subject or information of that type. It will be equally as valid if sent to anyone within the Trust.

If you receive a SAR, please contact dpo@dmat.education. A request for information does not need to mention that it is a SAR provided that it is clear that it is an individual asking for their own personal data. There is no specified wording, and it does not have to be on an official form. A SAR does not need to be in writing and can be made verbally, by post, by email or even using social media where relevant.

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 them 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, social media) or verbally (e.g., during a telephone conversation or meeting). 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 hold about me' would constitute a data subject access request (SAR) and should be treated as such.

A data subject is 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. This allows the Trust to easily recognise the SAR access request and the nature of the request. If the request is unclear/vague the Trust may be required to clarify the scope of the request which may in turn delay the start of the time for dealing with the request.

If a request is made verbally, the Trust will ensure that this is followed up with something in writing to confirm what has been requested and outline the time limit 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 dpo@dmat.education who should contact 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. If ever in doubt, please refer the request to dpo@dmat.education.

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.

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. In the case of 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 license, 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, but 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.

When it is necessary to verify the identity of the person making the request, the one calendar month period for responding begins when sufficient confirmation of identity is provided.

When it is necessary to request more information for the purpose of clarifying the request, the one calendar month period for responding pauses when further information is requested and does not restart until sufficient clarification is provided.

In both cases, the Trust will be unable to comply with the request if they do not receive the additional information.

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 considered, 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.

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 considering the administrative costs of providing the information.

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

Extending the time period of a SAR

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 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

Clarification: The statutory one-month timeframe for SARs continues to apply regardless of school closure periods. While closure periods may make collection slower, schools should acknowledge requests promptly, communicate timelines, and may extend by up to two months only where requests are complex or numerous. Closure periods alone do not automatically extend statutory deadlines.

A 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 we may not review

emails during this period and nobody will be onsite to deal with the request. As a result, it is unlikely that a request will be able to be dealt with during this time. A school may not be able to acknowledge a request during this time (i.e., until a time when we receive the request). However, if a school acknowledges the request, it may still not be able to deal with it until the school re-opens. A school will endeavour to comply with requests as soon as possible and will keep the requester updated as far as possible. If the request is urgent, it should be submitted 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 them 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, 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 Trust rectifies, erases, or restricts the processing of his personal data
    - 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 them together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for them

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 it 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 its 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
- safeguarding systems (such as CPOMS, My Concern;
- MIS system (Arbor)
- occupational health records
- pensions data
- share scheme information
- insurance benefit information

The Trust should search these systems using the individual's name, initials, 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 the relevant circumstances will be considered, including:

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

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 of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a 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 third parties for the purpose of actual or prospective:

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

Refusing to Respond to a Request

The Trust can refuse to comply with a request if the request in certain circumstances. These include:

- Where the SAR is manifestly unfounded or excessive, considering whether the request is repetitive in nature;
- To avoid obstructing an official or legal inquiry, investigation, or procedure;
- To avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- To protect public security;
- To protect national security;
- To protect the rights and freedoms of others.

If we decide not to comply with the SAR, then the data subject must be informed, without undue delay (and in all cases within one month of receipt of the request), of:

- The reasons we are not taking action;
- That they have a right to make a complaint to the ICO or another supervisory authority; and
- That they are entitled to seek to enforce their right through a judicial remedy. You must refer to dpo@dmat.education if you have concerns about supplying the information,

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 need to justify the decision and inform the requestor 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 do not need to comply with the request until the fee has been received.

Record Keeping

- A record of all subject access requests shall be kept by the dpo@dmat.education. 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- Subject Access Request Form

The Data Protection Act 2018 provides you, the data subject, with a right to receive a copy of the data/information we hold about you or to authorise someone to act on your behalf. Please complete this form if you wish to make a request for your data. Your request will normally be processed within one calendar month upon receipt of a fully completed form and proof of identity.

Proof of Identity

We require proof of your identity before we can disclose personal data. Proof of your identity should include a copy of a document such as your birth certificate, passport, driving licence, official letter addressed to you at your address e.g., bank statement, recent utilities bill or council tax bill. The document should include your name, date of birth and current address. If you have changed your name, please supply relevant documents evidencing the change.

Section 1

Please fill in the details of the data subject (i.e., the person whose data you are requesting). If you are not the data subject and you are applying on behalf of someone else, please fill in the details of the data subject below and not your own.

Title	
Surname/Family Name	
First Name(s)/ Forename(s)	
Date of Birth	
Address	
Post Code	
Phone Number	
Email address	

I am enclosing the following copies as proof of identity (please tick the relevant box):

Birth certificate	
Driving licence	
Phone Number	
An official letter to my address	

Personal Information *If you only want to know what information is held in specific records, please indicate in the box below. Please tell us if you know in which capacity the information is being held, together with any names or dates you may have. If you do not know exact dates, please give the year(s) that you think may be relevant.*
Details:

Employment record: If you are, or have been employed by the Trust and are seeking personal information in relation to your employment please provide details of your school, staff team, dates of employment etc. Details:

Section 2

Please complete this section of the form with your details if you are acting on behalf of someone else (i.e., the data subject).

If you are **NOT** the data subject, but an agent appointed on their behalf, you will need to provide evidence of your identity as well as that of the data subject and proof of your right to act on their behalf.

Title	
Surname/ Family Name	
First Name(s)/Forename(s)	
Date of Birth	
Address	
Post Code	

Phone Number	

I am enclosing the following copies as proof of identity (please tick the relevant box):

Birth certificate	
Driving licence	
Passport	
An official letter to my address	

What is your relationship to the data subject? (e.g., parent, carer, legal representative)

I am enclosing the following copy as proof of legal authorisation to act on behalf of the data subject	
Letter of authority	
Lasting or Enduring Power of Attorney	
Evidence of parental responsibility	
Other (give details):	

Section 3

Please describe as detailed as possible what data you request access to (e.g., time period, categories of data, information relating to a specific case, paper records, electronic records).

I wish to:
Receive the information by post*
Receive the information by email
Collect the information in person
View a copy of the information only
Go through the information with a member of staff

*Please be aware that if you wish us to post the information to you, we will take every care to ensure that it is addressed correctly. However, we cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household. Loss or incorrect delivery may cause you embarrassment or harm if the information is 'sensitive'.

Please send your completed form and proof of identity by email to: dpo@dmat.education

Appendix 3 – Data Use and Access Agreement (DUAA) – Template

Purpose and Scope

Describe the specific purpose(s) for accessing and using Trust data, the lawful basis under UK GDPR (e.g., public task, legal obligation, contract, consent, legitimate interests) and any special category/criminal offence conditions.

Parties and Roles

Identify the Parties and roles under UK GDPR (Controller-to-Controller or Controller-to-Processor). Include registered details and key contacts.

Data Description

List categories of personal data, data subjects, sources, and whether special category or criminal offence data is included.

Access Controls

Define role-based access, least privilege, MFA, encryption in transit and at rest, secure endpoints, and segregation of duties.

Permitted and Prohibited Uses

Specify only the agreed purposes. Prohibit onward disclosure, re-identification, marketing, or profiling not expressly authorised. No training of AI models on Trust data unless explicitly agreed in writing after a DPIA.

Sub-processors/Third Parties

Require prior written authorisation for any sub-processing and flow-down of equivalent obligations.

International Transfers

If data will leave the UK, state the applicable mechanism (Adequacy incl. UK–US Data Bridge, IDTA/UK Addendum, BCRs) and complete a Transfer Risk Assessment where required.

Security Measures

Reference minimum technical and organisational measures (TOMs) aligned to the Trust's Information Security Policy (e.g., patching, backups, logging/monitoring, vulnerability management, secure development).

Data Retention and Deletion

Define retention period(s), secure deletion/return on termination, and evidence of destruction.

Data Subject Rights

Processor to assist the Trust in responding to SARs, erasure, restriction, and objection requests within agreed SLAs.

Breach Notification

Immediate notification to the Trust on becoming aware of a personal data breach, with details to support ICO notification within 72 hours where required.

Audit and Assurance

Trust right to audit on notice; annual attestations; provision of relevant security certifications/ reports (e.g., ISO 27001, SOC 2) where available.

DPIA and Privacy by Design

Confirm whether a DPIA is required and completed; demonstrate privacy by design/default and Children's Code conformance where relevant.

Records and Accountability

Maintain records of processing activities (RoPA) and make them available on request.

Termination

On termination, cease processing, return or delete data as directed, and continue to protect any retained data required by law.

Liability and Indemnity

Set out liabilities for data protection breaches and allocation of risk between the Parties.

Governing Law and Jurisdiction

England and Wales unless otherwise agreed.

Signatures

Executed by authorised representatives of both Parties with date.