THE KITE ACADEMY TRUST

DATA PROTECTION POLICY

P1125

Contents

1 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 Kite Academy Trust will protect and maintain a balance between data protection rights in accordance with the UK GDPR. This policy sets out how the Trust 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 in order 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. Breach of this policy will be treated as a disciplinary offence which may result in action being taken in accordance with the Kite Academy Trust Disciplinary Procedure, up to and including summary dismissal depending on the seriousness of the breach.

2 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 the Trust possess or can reasonably access. 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 (e.g. 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 & 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.

3 When can Personal Data be processed?

Data Protection Principles

The Trust are responsible for and adhere 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, the Trust will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. The Trust will then regularly review those purposes whilst processing continues in order to be satisfied 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 the Trust's 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;
- 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 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;
- 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

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 School 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 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 the Trust 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 required by its obligations and duties. The Trust 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 also see the Kite Academy Trust Records Retention Policy.

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. The Trust 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.

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

Please also see the Kite Academy Trust Records Retention Policy.

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

In order to assure 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 (i.e. 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 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 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 (i.e. the Local Authority, Ofsted, the Department for Education or the Department of Health & Social Care). 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 with 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 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

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.

4 Data Subject's Rights & 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:

- To withdraw consent to processing at any time (where consent is relied upon as a condition of processing);
- Receive certain information about the Trust's processing activities;
- Request access to their personal data that is held by the Trust (see Appendix A - Subject Access Requests);
- Prevent use of their personal data by the Trust for marketing purposes;

- Ask the Trust 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;
- Restrict processing in specific circumstances;
- Challenge processing which has been justified on the basis of the Trust's legitimate interests or in the public interest;
- Request a copy of an agreement under which personal data is transferred outside of the EEA;
- Object to decisions based solely on automated processing;
- Prevent processing that is likely to cause damage or distress to the data subject or anyone else;
- Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
- Make a complaint to the supervisory authority (which is the Information Commissioner in England and Wales); and
- 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 are subject to certain rules and privacy laws when marketing. For example, a data subject's prior consent will be required for electronic direct marketing (i.e. 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 individuals. Specifically, employees must:

- Only access the personal data they 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 (e.g. 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 (i.e. pseudonymisation, encryption, password protection) to secure the information;
- Not store personal information on local drives.

5 Accountability

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

Data Protection Officer (DPO)

The Data Protection Officer for the Kite Academy Trust is **Judicium Consulting Limited**

Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB

Email: dataservices@judicium.com

Web: www.judiciumeducation.co.uk

Telephone: 0345 548 7000

The DPO is responsible for overseeing this Data Protection Policy and developing data-related policies and guidelines on behalf of the Trust.

Any questions or concerns regarding the implementation of this Data Protection Policy or the UK GDPR should be directed to the DPO.

In particular, contact must always be made with the DPO if:

- There is uncertainty of the lawful basis being relied on by the Trust to process personal data;
- Consent is to be relied upon as a fair reason for processing (see **Consent** above);
- There is a need to draft privacy notices or fair processing notices;
- There is uncertainty of the retention periods for the personal data being processed (see also The Kite Academy Trust Data Retention Policy);
- There is uncertainty of the security measures required to be put in place to protect personal data;
- A personal data breach has occurred (see the Kite Academy Trust Data Breach Procedure);
- There is uncertainty of the basis on which to transfer personal data outside the EEA;
- Assistance is required in dealing with any rights invoked by a data subject;
- A significant new (or a change in) processing activity is implemented which is likely to require a data protection impact assessment or if it is intended to use personal data for purposes other than what it was collected for;
- Activities involving automated processing or automated decision making are to be undertaken;
- Assistance is required in complying with applicable law when carrying out direct marketing activities;
- Assistance is required with 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). The Trust have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where the Trust are legally required to do so.

In the event that a personal data breach has occurred, or it is suspected a breach has occurred, contact should immediately be made with the Data Protection Officer.

Transparency and Privacy Notices

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 the data subject and set out information about how the Trust uses their data.

Whenever personal data is collected directly from data subjects, including for human resources or employment purposes, the Trust 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, how and why the Trust will use, process, disclose, protect and retain personal data. This information is provided within the Trust's privacy notices.

When personal data is collected indirectly (e.g. from a third party or a publicly available source), where appropriate, the Trust 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 adopt a privacy by design approach to data protection to ensure that data compliance is adhered to 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. To help 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)

In order to achieve a privacy by design approach, the Trust conduct 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).

The Trust's 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 school 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; and
- The risk mitigation measures in place and demonstration of compliance.

Record Keeping

The Trust are 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 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

The Trust will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws.

Audit

The Trust, through its Data Protection Officer, will regularly test its data systems and processes in order to assess compliance. This will be achieved through data audits which review the use of personal data.

Monitoring

The Trust will monitor the effectiveness of this and all of its policies and procedures, conducting full reviews and updates as appropriate.

The Trust's approach to monitoring and review will include consideration of how its policies and procedures are working in practice to reduce the risks posed to the Trust.

Document Management

Document ID:	P1125		
Last Review:	November 2024	**Review Period:**	3 years
Responsibility of:	Data Protection Officer	**Ratified by:**	Trustees (19.12.24)

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 the Trust is using their data and to check that it is being done 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:

- Confirmation that their data is being processed;
- Access to their personal data;
- A description of the information that is being processed;
- The purpose for which the information is being processed;
- The recipients/class of recipients to whom that information is or may be disclosed;
- 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 the Data Subject, 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 other supplementary information.

Dealing with a SAR is time critical and must be prioritised. Other than in exceptional cases, the Trust will have only 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 leave the Trust open 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 a member of staff receives a SAR they should contact the DPO (Judicium). 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 someone acting with the authority of an individual (i.e. 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
- Access to that personal data
- Certain other supplementary information

A valid SAR can be both in writing (e.g. letter, email, text message) 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 in order 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" will be 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, the Trust 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 a data subject access request and the nature of the request. If the request is unclear or vague, the Trust 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 **dpo@kite.academy** for advice to be sought from Judicium Consulting Ltd as the Trust's Data Protection Officer. There are limited timescales within which the Trust must respond to a request. Any delay could result in failing to meet the specified timescales, which could lead to enforcement action by the Information Commissioner's Office (ICO) and/or legal action by the affected individual. Failure to immediately report a data subject access request may result in disciplinary action being taken.

Acknowledging the Request

When receiving a SAR, the Trust shall acknowledge the request as soon as possible and inform the requester of 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 the DPO in order 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. In the case of current employees, this will usually be straightforward. The Trust is entitled to request additional information from a requester in order 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 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 information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child if individuals with parental responsibility cannot access this information; and
- any views the child 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 period of responding 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. Where the Trust may be required to get consent from a pupil, the time period will not start until consent is 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 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 Trust may not be able to respond to requests received during, or just before, school holidays within the one calendar month response period. This is because the academies within the Trust will be closed during these periods. As a result, it is unlikely that a request will be able to be dealt with during this time. The Trust may not be able to acknowledge the request during this time, however, if the Trust can acknowledge the request, it may still not be possible to deal with the request until academies re-open. The Trust will endeavour to comply with requests as soon as possible and will maintain communication with the requester as far as possible. If a request is urgent, it should be submitted during term times and not during, or close to, school closure periods.

Information to be Provided in Response to a Request

The individual is entitled to receive access to the personal data the Trust process about them and the following information:

- the purpose for which the Trust 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 Trust rectifies, erases or restricts the processing of an individual's 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 the Trust has taken about an individual together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for an individual.

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 are 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 have one month in which to respond, the Trust is permitted 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.

The Trust is therefore permitted 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 need 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, human resources system, finance 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);
- MIS system (such as RM Integris);
- occupational health records;
- pensions data;
- share scheme information;
- insurance benefit information.

The Trust will 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 any third parties. If third party 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 if doing so would disclose information relating to another individual (including information identifying the other individual as the source of 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 individuals consent, the Trust will consider all of the relevant circumstances including:

- the type of information that would be disclosed;
- any duty of confidentiality owed 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 individual 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, the DPO will 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 do 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 do 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; or
    - provision by the individual of any service

    This exemption does not apply to confidential references that the Trust receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (i.e. the person giving the reference), which means that the Trust must consider the rules regarding disclosure of third-party data set out above before disclosing the reference.
- *Legal professional privilege*: The Trust do not have to disclose any personal data which are subject to legal professional privilege.
- *Management forecasting*: The Trust do 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 do 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 in certain circumstances; these include:

- where the SAR is manifestly unfounded or excessive, taking into account 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.

In the event that there are concerns about supplying the information, the matter must always be referred to the DPO who will make the decision.

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

- the reasons we are not taking action;
- that they have the right to make a complaint to the ICO or another supervisory authority; and
- they are entitled to seek to enforce their right through a judicial remedy.

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 Trust. 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 Kite Academy Trust

The Data Protection Act 2018 provides a data subject with a right to receive a copy of the data/information that The Kite Academy Trust holds about them, or to authorise someone to act on their behalf. This form should be completed for a subject access request. The request will normally be processed within one calendar month upon receipt of a fully completed form and proof of identity. Proof of identity is required before the Trust can disclose personal data. Proof of your identity should include a copy of a document such as a birth certificate, passport, driving license, bank statement, recent utilities bill or council tax bill. The document provided should include name, date of birth and current address. If you have changed your name, please supply relevant documents evidencing the change.

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.			
First Name (s):		**Title:**	
Last Name:		**Date of Birth:**	
Address:			
Postcode:			
Telephone:			
Email:			

I am enclosing the following copies as proof of identity (please tick the relevant box):	
	Birth certificate
	Driving license
	Passport
	An official letter to my address

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.

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 role, location, dates of employment etc.

Please complete this section of the form with your details if you are acting on behalf of someone else (i.e. the data subject).			
First Name (s):		**Title:**	
Last Name:		**Date of Birth:**	
Address:			
Postcode:			
Telephone:			
Email:			

I am enclosing the following copies as proof of identity (please tick the relevant box):	
	Birth certificate
	Driving license
	Passport
	An official letter to my address
Relationship to Data Subject:	

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):

Please describe in as much detail as possible the data that is being requested (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 the information to be posted to you, the Trust will take every care to ensure that it is addressed correctly, however, the Trust cannot be held liable if the information is lost in the post, 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: dpo@kite.academy