



**DATA PROTECTION & SUBJECT ACCESS
REQUEST POLICY**

SEPTEMBER 2020

CONTENTS

SECTION	PAGE
1. Introduction	2
2. Definitions	2
3. Responsibilities	2
4. Data Protection Principles	3
5. Transfer of Data outside the EEA	6
6. Data Subject's rights and requests	6
7. Direct Marketing	7
8. Accountability	7
9. Data Protection Officer	7
10. Personal Data Breaches	8
11. Transparency and Privacy Notices	8
12. Privacy BY Design	8
13. Data Protection Impact Assessments (DPIA)	8
14. Record Keeping	9
15. Training	9
16. Audit	9
17. Monitoring	9
Appendix 1 – Subject Access Requests	10
Appendix 2 – Subject Access Request Form	16
Appendix 3 – Data Protection Impact Assessment (DPIA)	20

1. Introduction

The General Data Protection Regulation (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 Aspire Schools Trust (the "Trust") will protect and maintain a balance between data protection rights in accordance with the 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 in order to remain compliant with legal obligations.

2. Definitions

Personal data: 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 pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

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

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

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

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

Data Controller: The organisation storing and controlling such information 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 organising, amending, retrieving using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

Data Protection Impact Assessment (DPIA): DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

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

3. Responsibilities

The Headteacher of each school within the Aspire Schools Trust is responsible for ensuring data protection compliance within their setting. Day to day responsibilities for data protection (including liaising with the Trust's appointed Data Protection Officer) may be delegated by the Headteacher to another member of staff within their school.

All members of staff are required to familiarise themselves with the content of this policy and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence. This may result in disciplinary action under the Trust's Disciplinary Policy, up to and including summary dismissal, depending on the seriousness of the breach.

Members of staff may have access to the personal data of other members of staff, suppliers, parents or pupils in the course of their employment or engagement. Where this is the case, the Trust expects those members of staff to meet the Trust's data protection obligations to those individuals. Specifically, all members of staff must: -

- Only access the personal data that 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 (for example by complying with rules on access to school premises, computer access, password protection and secure file storage and destruction - please refer to the Trust's Information Security Policy for further details about our security processes);
- Not remove personal data or devices containing personal data from the School premises unless permission has been given and appropriate security measures are in place (such as pseudonymisation, encryption, password protection) to secure the information;
- Not store personal information on local drives.

4. 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 GDPR. These principles are:

- **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 of data as set out in the 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 where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject.

Special Category Data

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

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

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 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 requires a very clear and specific statement to be relied upon.

A data subject will have consented to the processing of their personal data if they clearly indicate agreement 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 able to easily withdraw consent to processing at any time and withdrawal must be promptly honoured.

If explicit consent is required, 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.

Records will be kept of consents obtained, in order to demonstrate compliance with consent requirements under the 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.

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 Data 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 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 safeguarding and security measures. This includes using measures such as: -

- Encryption;
- Pseudonymisation (this is where the Trust replaces information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure);
- Ensuring authorised access (i.e. that only people who have a need to know the personal data are authorised to access it);
- Adhering to confidentiality principles;
- Ensuring personal data is accurate and suitable for the process for which it is processed.

The Trust follows procedures and uses technologies to ensure security; and will regularly evaluate and test the effectiveness of these 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.

Full details on the Trust's security measures are set out in the Trust's Information Security Policy.

4. 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. These include if the third party: -

- Has a need to know the information for the purposes of providing the contracted services;
- 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;
- The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- The transfer complies with any applicable cross border transfer restrictions; and
- A fully executed written contract has been obtained, which contains GDPR approved third party clauses.

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 on to 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 with an organisation outside of the Trust shall be clearly defined within written notifications and the details/basis for sharing that data given.

5. Transfer of Data outside the European Economic Area (EEA)

The GDPR restricts data transfers to countries outside the EEA, in order to ensure that the level of data protection afforded to individuals by the 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 GDPR. All members of 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.

6. Data Subject's rights and requests

Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data.

The rights data subjects have in relation to how the Trust handle their personal data are set out below: -

- (a) (Where consent is relied upon as a condition of processing) To withdraw consent to processing at any time;
- (b) Receive certain information about the Trust's processing activities;
- (c) Request access to their personal data that we hold (see "Subject Access Requests" at 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; and
- (m) In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

If any request is made to exercise the rights above, it is a requirement for the designated member of staff responsible for data protection within each of the Trust's schools to verify the identity of the individual making the request.

7. 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 (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.

8. Accountability

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

9. Data Protection Officer (DPO)

Please find below details of the Trust appointed 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: 0203 326 9174
Lead Contact: Craig Stilwell

The DPO is responsible for overseeing this data protection policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this Data Protection Policy or the 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 in the first instance);
- (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.

10. Personal Data Breaches

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

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

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact dpo@aspire-school-trust.org or the appointed DPO using the contact details provided in section 9.

11. 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. Privacy notices set out information for data subjects about how the Trust uses their data and the Trust's privacy notices are tailored to suit the data subject.

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 GDPR including the identity of the data protection officer, the Trust's contact details, how and why we will use, process, disclose, protect and retain personal data. This will be provided in our privacy notice.

When personal data is collected indirectly (for example from a third party or publically available source), 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 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 GDPR

12. 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. 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.

13. Data Protection Impact Assessments (DPIAs)

In order to achieve a privacy by design approach, DPIAs are conducted for any new technologies or programmes being used within the Trust which could affect the processing of personal data. In any event a DPIA will be carried out when required by the 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;

- 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.

14. Record Keeping

Each school within the Trust is required to keep full and accurate records of data processing activities. These records include:

-

- The name and contact details of the School;
- 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.

15. Training

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

16. Audit

The Trust (through its appointed Data Protection Officer) regularly test its data systems and processes in order to assess compliance. These tests are conducted through data audits which take place annually, in order to review the Trust's use of personal data.

18. Monitoring

We will monitor the effectiveness of this and all of 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, in order to reduce the risks posed to the Trust and its schools.

Appendix 1 – Subject Access Requests

Under Data Protection Law, Data Subjects have a general right to find out whether we 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 we are undertaking.

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

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 sources of information obtained;
- (g) In relation to any Personal Data processed for the purposes of evaluating matters in relation to the Data Subject, that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct; and
- (h) Other supplementary information.

How to recognise a subject access request (SAR)

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 school processes personal data about him or her and, if so
- for access to that personal data
- and/or certain other supplementary information

A valid SAR can be both in writing (by letter, email, WhatsApp, text) or verbally (e.g. during a telephone conversation) to any member of staff. The request may refer to the 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 School 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, we encourage any individuals who wish to make such a request to complete the Subject Access Request form found in Appendix B. This allows us to easily recognise that you wish to make a data subject access request and the nature of your request. If the request is unclear/ vague we may be required to clarify the scope of the request which may in turn delay the start of the time period for dealing with the request.

What to do when you receive a data subject access request

Members of staff should immediately direct all data subject access requests to their Headteacher (or designated person) who will contact the Trust's appointed DPO in order to assist with the request and what is required.

Acknowledging the request

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

In addition to acknowledging the request, the school 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 school must clarify what address/email address to use when sending the requested information; and/or
- consent (if requesting third party data).

The school 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 school 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 school 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 school 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 school may ask the requester for more information in order to clarify the request, but the requester shall never be asked why the request has been made. The school shall let the requestor know as soon as possible if more information is needed before responding to the request.

In both cases, the period for responding begins when the additional information has been received. If the school do not receive this information, they will be unable to comply with the request.

Requests made by third parties or on behalf of children

The school need 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 school may also require proof of identity in certain circumstances.

If the school is in any doubt or has any concerns regarding 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, as to 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 school should consider whether the child is mature enough to understand their rights. If the school is confident that the child can understand their rights, then the school should usually respond directly to the child or seek their consent before releasing their information.

An assessment will be made as to whether 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, the assessment will take into account, some or all of the following factors:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;

- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

Generally, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 12 years of age or older, provided that the school 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 school will require the written authorisation of the child before responding to the requester. Alternatively, the school will provide the personal data directly to the child.

The school 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 school will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive, a fee may be requested to cover administrative.

If a request is considered to be manifestly unfounded or unreasonable the school will inform the requester why this is considered to be the case and advise that the school 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 school 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.

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

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

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

School closure periods

It may not be possible to respond to requests received during or just before school closure periods, within the one calendar month response period. This is because the school will be closed and there will be no staff on site to comply with the request. As a result, it is unlikely that such a request will be dealt with during this time. School may not even be able to acknowledge requests during this time (i.e. until a time when we receive the request). If, however, school can acknowledge the request, it will do so, but it may still not be able to deal with it until the school re-opens. The school will endeavour to comply with requests

as soon as possible and will keep in communication with you as far as possible. If your request is urgent, please provide your request during term times and not just prior to or during school closure periods.

Information to be provided in response to a request

The individual is entitled to receive access to the personal data we process about him or her. 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 school is required to supply in response to a SAR must be supplied with reference to the data in question at the time the request was received. However, as the school has one month in which to respond the school 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.

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

How to locate information

The personal data the school 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 school may need to search some or all 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 e.g. external payroll service providers;
- occupational health records held by the Occupational Health provider;
- pensions data held by the Teachers' Pension Scheme or Local Government Pension Scheme;
- data held externally by consultants engaged by the Trust that may hold data, e.g. consultants engaged to provide assistance with performance management and/or disciplinary and grievance procedures.

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

Protection of third parties - exemptions to the right of subject access

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

The school 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 school does not have to disclose personal data if this would involve disclosing information relating to another individual (including information identifying the other individual as the source of information), who can be identified from the information, unless:

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

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

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

In each case, a decision needs to be taken as to whether it is appropriate to disclose the information. 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 school disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the school 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 school 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 school 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 school 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; or
- provision by the individual of any service

This exemption does not apply to confidential references that the school 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 school must consider the rules regarding disclosure of third-party data (set out above) before disclosing the reference.

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

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

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

Refusing to respond to a request

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

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

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

In either case the school needs 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 school should contact the individual promptly and inform them. The school does 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 Headteacher (or designated other). The record shall include the date the SAR was received, the name of the requester, what data the School 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 Aspire Schools Trust holds 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 and send to Craig Stillwell, Data Protection Officer, Judicium Consulting Ltd, c/o Aspire Schools Trust, Main Road, Welbourn, LN5 0PA or electronically via email to dpo@aspire-schools-trust.org. Your request will normally be processed within one calendar month, upon receipt of a fully completed form and proof of identity.

Section 1 – Data Subject Details

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	
Forename(s)	
Date of Birth	
Address	
Post Code	
Phone Number	
Email address	
If you are a current or former employee of Aspire Schools Trust, please provide your employee identification number and your approximate dates of employment:	

Proof of identity: We require proof of your identity before we can respond to your access request. To help us establish your identity, you must provide identification that clearly shows your name, date of birth, and current address. We accept a photocopy or a scanned image of one of the following as proof of identity: passport or photo identification such as a driver's license, national identification number card, or birth or adoption certificate. Please also attach a copy of a bank or credit card statement or utility bill showing your current address and dated within the last three months. If you have changed your name, please provide the relevant documents evidencing the change.

If you do not have any of these forms of identification available, please contact to Craig Stillwell, Data Protection Officer, Judicium Consulting Ltd, c/o Aspire Schools Trust, Main Road, Welbourn, LN5 0PA or electronically via email to dpo@aspire-schools-trust.org

We may request additional information from you to help confirm your identity and your right to access, and to provide you with the personal data we hold about you. We reserve the right to refuse to act on your request if we are unable to identify you.

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

Section 2 – Authorised Person Details

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

Title	
Surname	
Forename(s)	
Date of Birth	
Address	
Post Code	
Phone Number	
Email address	
What is your relationship to the data subject? (e.g. parent, carer, legal representative)	

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. Proof of your identity should include a photocopy or a scanned image of one of the following as proof of identity: passport or photo identification such as a driver's license, national identification number card, or birth or adoption certificate. Please also attach a copy of a bank or credit card statement or utility bill showing your current address and dated within the last three months. If you have changed your name, please provide the relevant documents evidencing the change.

If you do not have any of these forms of identification available, please contact to Craig Stillwell, Data Protection Officer, Judicium Consulting Ltd, c/o Aspire Schools Trust, Main Road, Welbourn, LN5 0PA or electronically via email to dpo@aspire-school-trust.org

We may request additional information from you to help confirm your identity and your right to access, and to provide you with the personal data we hold about you. We reserve the right to refuse to act on your request if we are unable to identify you.

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

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 – Data request

Please describe, in as much detail as possible what data you request access to (time period/ categories of data/ information relating to a specific case/ paper records/ electronic records).

For example, you may specify that you are seeking:

- Employment records or personnel records.
- Personal data held by [DEPARTMENT].
- Medical records.
- E-mail or other electronic communications (specify the approximate dates and times).
- Billing information.
- Photographs.
- Video footage.
- User activity logs.
- Transaction histories
- Correspondence between [NAME] and [NAME] between [DATE] and [DATE].

We will contact you for additional information if the scope of your request is unclear or does not provide sufficient information for us to conduct a search (for example, if you request "all information about me"). We will begin processing your access request as soon as we have verified your identity and have all of the information we need to locate your personal data.

Section 4 – Data Subject Declaration

I confirm that the information provided on this form is correct and that I am the person whose name appears on this form. I understand that:

- Aspire Schools Trust must confirm proof of identity and may need to contact me again for further information;
- my request will not be valid until Aspire Schools Trust receives all of the required information to process the request; and
- I am entitled to one free copy of the personal data I have requested, and acknowledge that for any further copies I request, Aspire Schools Trust may charge a reasonable fee based on administrative costs.

Signature of Data Subject	
Date	

If you would like to receive a copy of the personal data you are requesting access to, please indicate below how you wish to receive this:

- by post*
- 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, we will take every care to ensure that it is addressed correctly to the data subject. 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'.*

Section 5 – Authorised Person Declaration

I confirm that I am authorised to act on behalf of the data subject. I understand that Aspire Schools Trust must confirm my identity and my legal authority to act on the data subjects behalf, and may need to request additional verifying information.

Signature of Authorised Person	
Date	

Please send your completed form and proof of identity by post to Craig Stillwell, Data Protection Officer, Judicium Consulting Ltd, c/o Aspire Schools Trust, Main Road, Welbourn, LN5 0PA or electronically via email to dpo@aspire-school-trust.org

Appendix 3 - Data Protection Impact Assessment (DPIA)

Please complete all sections and email the Data Protection Officer dataservices@judicium.co.uk for further guidance that should be considered. DPIA's must be reviewed annually to ensure continuing GDPR compliance.

School:	
Assessed by:	

Name of project/technology/system – *please provide a summary of the project/technology/system being used and how it impacts on personal data.*

--

Aims of the project/technology system – *please set out what the aims of the project/technology/system are and what are the anticipated benefits to school.*

--

Use of personal data – *please indicate if the project/technology/system involves the collection/use of personal data. If so, what data it collects, whether the data is particularly sensitive and whether any new data is collected as a result.*

--

Reason for processing – *please set out the reasons for processing including any fair processing conditions (such as consent of the individual, in order to comply with a contract, legal obligation, etc). This is to ensure compliance with Principle 1 of the data protection principles under GDPR. Also set out whether you intend to use this personal data for the purpose it is currently used or in a way that it is not currently used.*

--

Impact to personal data – *please indicate how the processing of personal data will be impacted by the use of the project/technology/system (such as how often you will be collecting data, how long will the data be kept, which individuals are affected).*

--

Risks to personal data – *please indicate the level of risk (i.e. low, medium, high) and set out the risks to individuals including:*

- *Risks on privacy (such as intrusion);*
- *Risks to the school such as compliance risks and costs;*
- *Risk to the information being shared inappropriately;*
- *Risks to collection, storing, sharing data; and*
- *Risks to vulnerable people/sensitive information.*

--

Will this personal data be shared with third parties? – *if 'yes', please indicate which third parties will receive personal data, which personal data the third party will receive and the reason the third party will receive the personal data.*

--

What steps will be taken to protect the personal data? – please indicate all measures to be taken to protect the personal data, for example:

- Security measures;
- Agreements in place;
- Any consultation that has taken place on the project/technology/system;
- Steps taken to destroy personal data when no longer needed;
- Training/awareness raising amongst staff and other individuals;
- If personal data can be anonymised;
- Providing guidance to others;
- Transparency with individuals; and
- Necessity of processing.

Please note if the information is particularly sensitive or to be shared it with third parties, please indicate this and set out additional steps being taken to protect the sensitive data.

Any other factors to consider?

Assessor Compliance Statement

I confirm that this DPIA has been completed to the best of my knowledge and complies with the data protection principles under the GDPR. All privacy risks have been considered and represent a proportionate response to the identified risks to personal data.

Name:

Signature:

Date:

DPO Statement

I can confirm that I have reviewed the DPIA above and are satisfied that the school have taken appropriate and proportionate steps to protect the data.

Name:

Signature:

Date: