Data Protection Policy

Approved by Board of Directors:	**10 July 2025**
Revision date:	**July 2026**
Version:	**4.0**

Contents

Data Protection Policy

1. Aims

Aspire Multi-Academy Trust (MAT) academies aim to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of:

- The UK General Data Protection Regulation (UK GDPR), which replaced the EU GDPR in the UK post-Brexit. References to EU GDPR now apply only where data is processed in the EU."
- The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

It also reflects the ICO's guidance for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and Articles of Association.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data, which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes

	• Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
Artificial Intelligence (AI)	Technologies that perform tasks typically requiring human intelligence, such as decision-making, data analysis, content generation, or personalisation.

4. The Data Controller – Aspire MAT

Aspire academies processes personal data relating to parents, pupils, staff, governors, visitors and others. Aspire MAT is therefore registered as the data controller with the ICO, with individual academies added as 'trading names' of the MAT.

5. Roles and responsibilities

This policy applies to **all staff** employed by Aspire and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing Board

The governing board of each academy has responsibility for ensuring that their academy complies with all relevant data protection obligations. The MAT board has overall responsibility for ensuring compliance across all academies and our central functions.

5.2 Data Protection Officer

Each academy's data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable. In this role, academy DPOs are supported by the OHRO of Aspire, who serves as DPO for the central functions of the MAT. The DPO acts independently and reports directly to the Board of Trustees, in accordance with Article 38 of UK GDPR. The Trust ensures that the DPO has sufficient resources, authority, and access to carry out their duties objectively

DPOs will provide an annual report of their activities directly to both the governing board of their academy and the MAT board, presenting their advice and recommendations on academy data protection issues.

DPOs are the first point of contact for individuals whose data the academy processes and for the ICO. In Aspire academies, the DPOs are detailed in Appendix 7.

Each Aspire academy DPO – as well as MAT DPO – will conduct an annual **Data Protection Audit**, for which there is an Excel template.

5.3 Headteacher

The headteacher of each academy acts as the representative of the data controller on a day-to-day basis.

5.4 All Staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Seek approval before using an AI tools involving personal data and avoid inputting any personal or sensitive data into unauthorised and unapproved technologies
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - When a DPIA is required and completing the process for sign-off
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The UK GDPR is based on data protection principles that Aspire academies must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how Aspire academies aim to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the academy can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the academy can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual or another person e.g. to protect someone's life
- The data needs to be processed so that the academy, as a public authority, can perform a task **in the public interest or exercise its official authority** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the academy (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden.
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent

- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the MAT retention schedule.

8. Sharing Personal Data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law
    - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the academy holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this is not possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests must be submitted in writing, either by letter or email to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child
- Would include another person's personal data that we can't reasonably anonymise, and we do not have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee which takes into account administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their data is transferred to a country outside the UK. Where such transfers occur, the Trust will ensure they are based on UK adequacy regulations or safeguarded by appropriate legal mechanisms, such as Standard Contractual Clauses.
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)

- Prevent processing that is likely to cause damage or distress
- Object to processing that has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see educational records

In academies – as opposed to maintained schools – parents, or those with parental responsibility, do not have an automatic legal right of access to their child's educational record (which includes most information about a pupil). However, Aspire academies will consider all such requests within 15 school days of a written request being received.

11. CCTV

Aspire academies use CCTV in various locations to help ensure site safety. We will follow the ICO's guidance for the use of CCTV and comply with data protection principles.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed, in the first instance, to the academy DPO.

12. Photographs and videos

As part of academy activities, staff may take photographs and record images of individuals.

Aspire academies will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Any photographs and videos taken by parents/carers at academy events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Uses may include:

- Within each academy on notice boards and in magazines, brochures, newsletters, etc.
- Outside of the academy by external agencies such as the school photographer, newspapers, campaigns
- Online on academy or MAT websites or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child to ensure they cannot be identified.

13. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. Aspire Multi-Academy Trust recognises that AI has many uses to help pupils learn but also poses risks to sensitive and personal data.

In light if this Aspire Multi-Academy Trust recognises the increasing use of artificial intelligence (AI) in educational and administrative settings. We have therefore produced an Aspire AI Policy for further clarification.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Aspire Multi-Academy Trust will treat this as a data breach, and will follow the personal data breach procedure outlined in Appendix 1.

Where automated processing or decision-making is used:

- A Data Protection Impact Assessment (DPIA) must be completed before use of any AI
- No significant decisions about individuals will be made solely by automated means, in line with Article 22 of UK GDPR
- The Trust's AI & Emerging Technologies Policy must be followed
- AI tools must be authorised and listed in the school's AI Tool Register
- School level logs must be kept and monitored for high-risk applications

14. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply

- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure.

15. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment. See academy specific online safety policy / ICT policy / acceptable use agreement / policy on acceptable use.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

16. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal data breaches

The Trust and our academies will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in an academy context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

18. Training

All staff and governors are required to complete data protection training as part of their induction process. Ongoing training also forms part of Aspire Multi-Academy Trust's commitment to continuing professional development, particularly where changes to legislation, statutory guidance, or internal Trust and school procedures make it necessary.

Aspire MAT subscribes to The Key for School Leaders, providing all staff with access to up-to-date online training and resources on data protection and related compliance areas. Designated Data Protection Officers (DPOs) additionally have access to the DPO Resource Hub, which supports their oversight responsibilities across the Trust.

For directors, trustees and governors, training and updates on data protection responsibilities are available via GovernorHub – Knowledge, which the Trust uses to support Local Governing Bodies (LGBs) in understanding their legal obligations and good practice in information governance.

19. Monitoring arrangements

Academy DPOs – together with the MAT DPO – are responsible for monitoring and reviewing this policy, which will be presented to the MAT Board on an annual basis.

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the academy DPO.
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the headteacher and the MAT Operations and HR Officer (OHRO). Depending on the seriousness of the breach, the headteacher may wish to alert the Chair of Governors. Breaches which require reporting to the ICO will always be discussed with the Chair.
- Staff, trustees and governors will co-operate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure).
- The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences.
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool.
- The DPO will document the decision (either way) in case it is challenged at a later date by the ICO or an individual affected by the breach.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website or through its breach report line (0303 123 1113), within 72 hours of the academy's awareness of the breach. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned;
        - The categories and approximate number of personal data records concerned.
    - The name and contact details of the DPO;
    - A description of the likely consequences of the personal data breach;
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the academy's awareness of the breach. The report will explain that there is a delay,

the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach;
    - The name and contact details of the DPO;
    - A description of the likely consequences of the personal data breach;
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.
- The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

  Records of all breaches will be stored centrally by the MAT OHRO.
- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.
- The Academy DPO and headteacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches.

Action to minimise the impact of data breaches

We will take action to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach. Academy DPOs – in consultation with the MAT DPO and OHRO – will determine which actions to take to mitigate impact. The examples below apply to one type of data breach – accidental disclosure via email.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the academy DPO as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the academy DPO will ask the ICT support to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence).
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the academy DPO will consider whether it is appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request

that those individuals delete the information and do not share, publish, save or replicate it in any way.

- The academy DPO will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.
- The academy DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners.

Appendix 2: Model privacy notice for parents/carers

Privacy notice for parents/carers

Under data protection law, individuals have a right to be informed about how the academy uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about parents and carers of pupils at our academy.

Aspire Multi-Academy Trust is the 'data controller' for the purposes of UK data protection law.

Our academy Data Protection Officer (DPO) is ……

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details and contact preferences (such as your name, address, email address and telephone numbers);
- Bank details;
- Details of your family circumstances;
- Details of any safeguarding information including court orders or professional involvement;
- Records of your correspondence and contact with us;
- Details of any complaints you have made;
- Information about your use of our information and communication systems, equipment and facilities (e.g. school computers).

We may also collect, use, store and share (when appropriate) information about you that falls into 'special categories' of more sensitive personal data. This includes, but is not restricted to:

- Information about any health conditions you have that we need to be aware of;
- Photographs and CCTV images captured in school;
- Information about your religion, as part of our admissions arrangements.

We may also hold data about you that we have received from other organisations, including other schools and social services.

Why we use this data

We use the data listed above to:

- Report to you on your child's attainment and progress;
- Keep you informed about the running of the school (such as emergency closures) and events;
- Process payments for school services and clubs;
- Provide appropriate pastoral care;
- Protect pupil welfare;
- Administer admissions waiting lists;
- Assess the quality of our services;

- Carry out research;
- Comply with our legal and statutory obligations;
- Make sure our information and communication systems, equipment and facilities (e.g. school computers) are used appropriately, legally and safely.

Use of your personal data for marketing purposes

Where you have given us consent to do so, we may send you marketing information by email or text promoting school events, campaigns, charitable causes or services that may be of interest to you.

You can withdraw consent or 'opt out' of receiving these emails and/or texts at any time by contacting the academy office.

Use of your personal data in automated decision making and profiling

We do not currently process any parents' or carers' personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the process to you, including your right to object to it.

Use of your personal data for filtering and monitoring purposes

While you are in our school, we may monitor your use of our information and communication systems, equipment and facilities (e.g., school computers). We do this so that we can:

- Comply with health and safety and other legal obligations;
- Comply with our policies (e.g., child protection policy, IT acceptable use policy) and our legal obligations;
- Keep our network(s) and devices safe from unauthorised access and prevent malicious software from harming our network(s).

Appendix 3: Model Privacy notice for the Aspire Multi-Academy Trust workforce

Privacy notice for our workforce

Under UK data protection law, individuals have a right to be informed about how the Trust uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work at our school.

ASPIRE MAT is the 'data controller' for the purposes of data protection law.

Our academy **Data Protection Officer** (DPO) is …….

The personal data we hold

We process data relating to those we employ, or otherwise engage, to work at our school. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details;
- Date of birth, marital status and gender;
- Next of kin and emergency contact numbers;
- Salary, annual leave, pension and benefits information;
- Bank account details, payroll records, National Insurance number and tax status information;
- Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process;
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships;
- Performance information;
- Outcomes of any disciplinary and/or grievance procedures;
- Absence data;
- Copy of driving licence;
- Photographs;
- CCTV footage;
- Data about your use of the school's information and communications systems, equipment and facilities (e.g. school computers).

We may also collect, use, store and share (when appropriate) information about you that falls into "special categories" of more sensitive personal data. This includes. but is not restricted to:

- Information about any health conditions you have that we need to be aware of;
- Sickness records;
- Photographs and CCTV images captured in school;
- Information about trade union membership.

We may also collect, use, store and share (when appropriate) information about criminal convictions and offences.

We may also hold data about you that we have received from other organisations, including other schools and social services, and the Disclosure and Barring Service in respect of criminal offence data.

Why we use this data

The purpose of processing this data is to help us run the school, including to:

- Enable you to be paid;
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils;
- Support effective performance management;
- Inform our recruitment and retention policies;
- Allow better financial modelling and planning;
- Enable equalities monitoring;
- Improve the management of workforce data across the sector;
- Support the work of the School Teachers' Review Body;
- Make sure our information and communications systems, equipment and facilities (e.g. school computers) are used appropriately, legally and safely.

Use of your personal data for marketing purposes

Where you have given us consent to do so, we may send you marketing information by email or text promoting school events, campaigns, charitable causes or services that may be of interest to you.

You can withdraw consent or 'opt out' of receiving these emails and/or texts at any time by contacting the academy office.

Use of your personal data in automated decision making and profiling

We do not currently process any staff members' personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

Use of your personal data for filtering and monitoring purposes

While you are in our school, we may monitor your use of our information and communication systems, equipment and facilities (e.g. academy computers). We do this so that we can:

- Comply with health and safety and other legal obligations;
- Comply with our policies (e.g. child protection policy, IT acceptable use policy) and our legal obligations;
- Keep our network(s) and devices safe from unauthorised access and prevent malicious software from harming our network(s).

Our lawful basis for using this data

Our lawful bases for processing your personal data for the purposes listed in section 3 above are as follows:

- For the purposes of and in accordance with the 'public task' basis – we need to process data to fulfil our statutory function as an academy.
- For the purposes of and in accordance with the 'legal obligation' basis – we need to process data to meet our responsibilities under law.

- For the purposes of and in accordance with the 'consent' basis – we will obtain consent from you to use your personal data.
- For the purposes of and in accordance with the 'vital interests' basis – we will use this personal data in a life-or-death situation.
- For the purposes of and in accordance with the 'contract' basis – we need to process personal data to fulfil a contract with you or to help you enter into a contract with us.
- For the purposes of in accordance with the 'legitimate interests' basis – where there's a minimal privacy impact and we have a compelling reason.

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent and explain how you will go about withdrawing consent if you wish to do so.

Our basis for using special category data

For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and 1 of the following conditions for processing as set out in UK data protection law:

- We have obtained your explicit consent to use your personal data in a certain way.
- We need to perform or exercise an obligation or right in relation to employment, social security or social protection law.
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you are physically or legally incapable of giving consent.
- The data concerned has already been made manifestly public by you.
- We need to process it for the establishment, exercise or defence of legal claims.
- We need to process it for reasons of substantial public interest as defined in legislation.
- We need to process it for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law.
- We need to process it for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law.
- We need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest.

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in UK data protection law. Conditions include:

- We have obtained your consent to use it in a specific way.
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you are physically or legally incapable of giving consent.
- The data concerned has already been made manifestly public by you.
- We need to process it for, or in connection with, legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights.
- We need to process it for reasons of substantial public interest as defined in legislation.

Collecting this information

While the majority of information we collect from you is mandatory, there is some information that. can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Most of the data we hold about you will come from you, but we may also hold data about you from:

- Local authorities;
- Government departments or agencies;
- Police forces, courts or tribunals.

How we store this data

We keep personal information about you while you work at our school. We may also keep it beyond your employment at our school if this is necessary. Our record retention schedule sets out how long we keep information about staff.

A copy of our record retention schedule can be found on the Aspire Multi-Academy Website: https://www.aspire-mat.co.uk/mat-policies/

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your personal data securely when we no longer need it.

Data sharing

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with UK data protection law) we may share personal information about you with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns;
- The Department for Education;
- Other Government departments or agencies;
- Your family or representatives;
- Educators and examining bodies;
- Our regulator [e.g. Ofsted/SIAMS];
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as payroll;
- Financial organisations;
- Our auditors;
- Survey and research organisations;
- Trade unions and associations;
- Health authorities;
- Security organisations;
- Health and social welfare organisations;
- Professional advisers and consultants;
- Charities and voluntary organisations;
- Police forces, courts, tribunals;

- Professional bodies;
- Employment and recruitment agencies.

Transferring data internationally

Where we transfer your personal data to a third-party country or territory, we will do so in accordance with UK data protection law.

In cases where we have to set up safeguarding arrangements to complete this transfer, you can get a copy of these arrangements by contacting us.

Your rights

a. How to access personal information we hold about you

You have a right to make a 'subject access request' to gain access to personal information that we hold about you.

If you make a subject access request, and if we do hold information about you, we will (subject to any exemptions that may apply):

- Give you a description of it;
- Tell you why we are holding and processing it, and how long we will keep it for;
- Explain where we got it from, if not from you;
- Tell you who it has been, or will be, shared with;
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this;
- Give you a copy of the information in an intelligible form.

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact your academy data protection officer.

b. Your other rights regarding your data

Under UK data protection law, you have certain rights regarding how your personal data is used and kept safe. For example, you have the right to:

- Object to our use of your personal data;
- Prevent your data being used to send direct marketing;
- Object to and challenge the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person);
- In certain circumstances, have inaccurate personal data corrected;
- In certain circumstances, have the personal data we hold about you deleted or destroyed, or restrict its processing.
- Withdraw your consent, where you previously provided it for the collection, processing and transfer of your personal data for a specific purpose;
- In certain circumstances, be notified of a data breach;
- Make a complaint to the Information Commissioner's Office;
- Claim compensation for damages caused by a breach of the data protection regulations;

To exercise any of these rights, please contact the academy data protection officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/make-a-complaint/ ;
- Call 0303 123 1113;
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact your academy data protection officer.

Appendix 4: Model privacy notice for pupils

Privacy notice for Pupils

You have a legal right to be informed about how our school uses any personal information that we hold about you. To comply with this, we provide a 'privacy notice' to you where we are processing your personal data.

This notice explains how we collect, store and use personal data about pupils at our school, like you.

Aspire Multi Academy Trust is the 'data controller' for the purposes of UK data protection law.

Our academy data protection officer (DPO) is ……..

The personal data we hold

We hold some personal information about you to make sure we can help you learn and look after you at school.

For the same reasons, we get information about you from some other places too – such as other schools, the local council and the government.

Personal information that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Your contact details
- Your test results
- Your attendance records
- Details of any behaviour issues or exclusions
- Information about how you use school computers and other IT and communications systems

We may also collect, use, store and share (when appropriate) information about you that falls into 'special categories' of more sensitive personal data. This includes, but is not restricted to:

- Information about your characteristics, like your ethnic background or any special educational needs
- Information about any medical conditions you have
- Photographs and CCTV images
- Eligibility for free school meals
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Other data received from other organisations, including other schools, local authorities and the Department for Education.

Why we use this data

We use the data listed above to:

- Get in touch with you and your parents or carers when we need to
- Check how you are doing in exams and work out whether you or your teachers need any extra help

- Track how well the school as a whole is performing
- Look after your wellbeing
- Make sure our computers and other school systems and equipment are used appropriately, legally and safely

Use of your personal data for marketing purposes

Where you have given us consent to do so, we may send you messages by email or text promoting school events, campaigns, charitable causes or services that you might be interested in.

You can take back this consent or 'opt out' of receiving these emails and/or texts at any time by contact the academy office.

Use of your personal data in automated decision making and profiling

We do not currently put pupils' personal data through any automated decision making or profiling process. This means we do not make decisions about you using only computers, without any human involvement.

Use of your personal data for filtering and monitoring purposes

While you are in school, we may monitor what material you access on our computers and other IT and communication systems. We do this so that we can:

- Comply with health and safety law and other laws
- Comply with our policies (e.g. child protection policy, IT acceptable use policy)
- Keep our network(s) and devices safe from people who are not allowed to access them, and prevent harmful software from damaging our network(s)
- Protect your welfare

Our lawful basis for using this data

We will only collect and use your information when the law allows us to. We need to establish a 'lawful basis' to do this.

Our lawful bases for processing your personal information for the reasons listed in section 3 above are:

- For the purposes of and in accordance with the 'public task' basis – we need to process data to fulfil our official duties as an academy.
- For the purposes and in accordance with the 'legal obligation' basis – we need to process data to meet our responsibilities under law.
- For the purposes of and in accordance with the 'consent' basis – we will get consent from you to use your personal data
- For the purposes of and in accordance with the 'vital interests' basis – we will use this personal data in a life-or-death situation
- For the purposes of and in accordance with the 'contract' basis – we need to process personal data to fulfil a contract with you or to help you enter into a contract with us
- For the purposes of and in accordance with the 'legitimate interests' basis – where there is a minimal privacy impact and we have a compelling reason.

Where you have agreed that we are allowed to use your information ('given consent'), you may take this back at any time. We will make this clear when requesting your consent, and explain how you would go about withdrawing consent if you want to.

Our basis for using special category data

For 'special category' data (more sensitive personal information), we only collect and use it when we have both a lawful basis, as set out above, and 1 of the following conditions for processing as set out in UK data protection law:

- We have your explicit consent to use your information in a certain way
- We need to use your information under employment, social security or social protection law
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you are physically or legally incapable of giving consent
- The information has already been made obviously public by you
- We need to use it to make or defend against legal claims
- We need to use it for reasons of substantial public interest as defined in legislation
- We need to use it for health or social care purposes, and it is used by, or under the direction of, a professional obliged to confidentiality under law
- We need to use it for public health reasons, and it is used by, or under the direction of, a professional obliged to confidentiality under law
- We need to use it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the use is in the public interest

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in UK data protection law. Conditions include:

- We have your consent to use it in a specific way
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you are physically or legally incapable of giving consent
- The data concerned has already been made obviously public by you
- We need to use it as part of legal proceedings, to obtain legal advice, or to make or defend against legal claims
- We need to use it for reasons of substantial public interest as defined in legislation

Collecting this data

While most of the information we collect about you is mandatory (i.e. you have to give us the information), there is some information that you can choose whether or not to give us.

Whenever we want to collect information from you, we make it clear whether you have to give us this information (and if so, what the possible consequences are of not doing that), or whether you have a choice.

Most of the data we hold about you will come from you or your parents, but we may also hold data about you from:

- Local councils
- Government departments or agencies
- Police forces, courts or tribunals

How we store this data

We keep personal information about you while you are attending our school. We may also keep it after you stop attending our school, if this is necessary. Our record retention schedule sets out how long we keep information about pupils.

A copy of our record retention schedule can be found on the Aspire Multi-Academy Website: https://www.aspire-mat.co.uk/mat-policies/

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your personal data securely when we no longer need it.

Who we share data with

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with UK data protection law), we may share personal information about you with:

- Our local authority, [name of local authority] – because we have to share certain information with it, such as safeguarding concerns and information about exclusions
- Government departments or agencies
- Our youth support services provider
- Our regulator, [specify as appropriate, e.g. Ofsted, Independent Schools Inspectorate]
- Suppliers and service providers:
- List the specific types of providers (e.g. catering, filtering and monitoring)
- Financial organisations
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts or tribunals

National Pupil Database

We have to provide information about you to the Department for Education (a government department) as part of data collections such as the school census.

Some of this information is then stored in the National Pupil Database, which is managed by the Department for Education and provides evidence on how schools are performing. This, in turn, supports research.

The database is held electronically so it can easily be turned into statistics. The information it holds is collected securely from schools, local authorities, exam boards and others.

The Department for Education may share information from the database with other organisations, such as organisations that promote children's education or wellbeing in England. These organisations must agree to strict terms and conditions about how they will use your data.

You can find more information about this on the Department for Education's webpage on how it collects and shares personal data.

You can also contact the Department for Education if you have any questions about the database.

Transferring data internationally

We may share personal information about you with the following international third parties (organisations, companies etc, that are based outside the UK), where different data protection legislation applies:

[Insert the relevant organisations and countries, and for each one explain whether you transfer data on the basis of an adequacy regulation (previously named 'adequacy decision') by the UK government, or if you have set up your own safeguards]

Where we transfer your personal data to a third-party country or territory, we will follow UK data protection law.

In cases where we have to set up safeguarding arrangements to complete this transfer, you can get a copy of these arrangements by contacting us.

Your rights

How to access personal information that we hold about you

You have a right to make a 'subject access request' to gain access to personal information that we hold about you.

If you make a subject access request, and if we do hold information about you, we will (unless there is a really good reason why we should not):

- Give you a description of it
- Tell you why we are holding and using it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data (decisions made by a computer or machine, rather than by a person), and any consequences of this
- Give you a copy of the information in an understandable form

You may also have the right for your personal information to be shared with another organisation in certain circumstances.

If you would like to make a request, please see appendix 7 for our template and contact your academy DPO.

Your other rights regarding your data

Under data protection law, you have certain rights regarding how your personal information is used and kept safe. For example, you have the right to:

- Say that you do not want your personal information to be used
- Stop it being used to send you marketing materials
- Say that you do not want it to be used for automated decisions (decisions made by a computer or machine, rather than by a person)
- In some cases, have it corrected if it is inaccurate
- In some cases, have it deleted or destroyed, or restrict its use
- Withdraw your consent, where you previously provided consent for your personal information to be collected, processed and transferred for a particular reason
- In some cases, be notified of a data breach

- Make a complaint to the Information Commissioner's Office
- Claim compensation if the data protection rules are broken and this harms you in some way

To exercise any of these rights, please contact your academy DPO.

Complaints

We take any complaints about how we collect and use personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concerns about our data processing, please let us know first.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/make-a-complaint/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions or concerns, or would like more information about anything mentioned in this privacy notice, please contact your academy data protection officer:

[Name and contact details of your data protection officer]

NB: You are required to include the details of your data protection officer in your privacy notice.

Appendix 5: Template letter to suppliers to ensure GDPR compliance

It is the role of the academy DPO to obtain addresses of any suppliers with whom personal data is shared and to contact them to obtain their assurance of UK GDPR compliance. The template below is suggested for this purpose.

Dear [third party/supplier],

Re: Compliance with the UK General Data Protection Regulation

We are conducting due diligence on all suppliers with whom we share individuals' personal data to make sure that they, and therefore we, are compliant.

We would appreciate it if you could answer the following questions to help us do this:

1. What technical and organisational security measures do you have in place to protect personal data?
2. What policies and procedures do you have in place to protect personal data?
3. How secure are your systems?
4. Do you have any information management accreditation?

We also need to ensure that the contract we have with you reflects the UK GDPR, and is updated to include:

- The subject matter, duration, nature and purpose of the processing
- The type of personal data being processed
- The categories of the data subjects
- Our obligations and rights as the data controller
- That the data processer (you, the third party/supplier) processes data only on the documented instructions of the school
- That the people who process the data are committed to confidentiality
- That you take measures to ensure secure processing
- That you will not engage another processor without prior written authorisation from the school, and that if you do so, that processor will also be bound by the same data protection conditions as are in your contract with us
- That you help the school comply with requirements regarding the data rights of individuals (e.g., to access, delete or rectify data), secure processing, the reporting and communication of data breaches, and the conducting of impact assessments where relevant
- *[If applicable]* That you delete or return the personal data to the school at the end of your provision of services
- That you make information available to us to demonstrate your compliance with the obligations in our contract, and allow us or a third party instructed by us to conduct audits and inspections

Kindly confirm that you are willing to meet or speak with us to arrange the updating of our contract, and we will be in touch in due course.

Alternatively, if you have a privacy notice to send us which covers all of the above points, that would suffice.

Yours sincerely,

Appendix 6: Data Protection Impact Assessments (DPIAs)

Deciding if you need an DPIA:

The ICO explains that you must carry out a DPIA when:

- Using new technologies; and
- The processing is likely to result in a high risk to the rights and freedoms of individuals

3 types of processing will always require a DPIA that is likely to result in a high risk includes (but is not limited to):

- Systematic and extensive processing activities, including profiling and where decisions have legal effects, or similarly significant effects, on individuals
- Large-scale processing of special categories of data or personal data relating to criminal convictions or offences
- Large-scale, systematic monitoring of public areas (such as CCTV)

These are set out in article 35(3) of the UK GDPR

DPIAs must be conducted for AI tools, especially those using pupil or staff data in accordance with the Aspire AI Policy. Even for third-party tools integrated into platforms (e.g., MIS with AI features).

All DPIAs must be reviewed by the Data Protection Officer and signed off by The Headteacher (as the Data Controller) to ensure any required mitigations are implemented before the processing begins. This process must be documented and logged in school.

Who should be involved in the DPIA?

Inform the Aspire Multi-Academy Trust DPO and OHRO centrally if a DPIA is required.

Anyone who is responsible for making decisions on data processing can carry out a DPIA.

It is for data controllers (Headteachers) to determine whether a DPIA is required.

Where AI or automated decision-making is introduced, a DPIA is mandatory and must consider risks related to data bias, accuracy, transparency, and safeguarding

Your data protection officer (DPO) **should not** carry out the assessment. They need to independently scrutinise the process.

The DPO should:

- Consult on the progress of the assessment
- Check your compliance with regulations
- Make recommendations about whether the data processing activity can go ahead

You might also need to consult:

- Information security staff
- Any processors
- Legal advisors or other independent experts, where relevant

How to carry out a DPIA

Follow the ICO's step-by-step guide to carrying out a DPIA.

- Identify the need for a DPIA
- Describe the processing
- Consider consultation

- Assess necessity and proportionality
- Identify and assess risks
- Identify measures to mitigate the risks
- Sign off and record outcomes
- ICO DPIA Template

Appendix 7: Subject access request template – for use of parents/carers and staff

Re: subject access request

Dear …… [insert name of your academy's Data Protection Officer

Please provide me with the information about me that I am entitled to under the UK General Data Protection Regulation. This is so I can be aware of the information you are processing about me and verify the lawfulness of the processing.

Here is the necessary information:

Name	
Relationship with the school	Please select: Pupil / parent / employee / governor / volunteer Other (please specify):
Correspondence address	
Contact number	
Email address	
Details of the information requested	Please provide me with: *Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:* • *Your personnel file* • *Your child's medical records* • *Your child's behaviour record, held by [insert class teacher]* • *Emails between 'A' and 'B' between [date]*

If you need any more information from me, please let me know as soon as possible.

Please bear in mind that under the UK GDPR you cannot charge a fee to provide this information, and in most cases, must supply me with the information within 1 month.

If you need any advice on dealing with this request, you can contact the Information Commissioner's Office on 0303 123 1113 or at www.ico.org.uk

Yours sincerely,

Name

Appendix 8: Academy Data Protection Officers (DPO)

In Aspire academies, the DPOs are as follows:

Archbishop Cranmer C of E Academy:	Eleanor Hodgson
East Bridgford St. Peter's C of E Academy:	Allison Gibbens
Gunthorpe C of E Primary School:	Paula Findlay
Kirkby Woodhouse Primary School:	Paul Stimpson
Langar C of E Primary School	David Owen-Jones
Sir John Sherbrooke Junior School:	Jenny Grant
Oak Tree Primary School & Nursery:	Ella Tuxford-Flory
Winthorpe Primary School:	Kelly Beanland