ASPIRE
Academies Trust

GDPR - Data Protection and Freedom of Information Policy

Reviewed: Autumn 2023 Review Frequency: Annually

Approved by the Board of Trustees

Contents:

DATA PROTECTION:

1. Introduction

Aspire Academies Trust processes personal data relating to parents, pupils, staff, governors, visitors, and others, and therefore is a data controller.

- The Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required to support its pupils' teaching and learning.
- Monitor and report on their progress.
- Provide appropriate pastoral care, and
- Assess how the Trust and the Academies as a whole are doing.

Because of this data collection, the academy has a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO). The type of information held by the trust, and its use, is available on the ICO's website. Aspire Academies Trust also have a duty to issue a Privacy Notice to all pupils/parents, this summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

Related documents

- Complaints policy
- ICT Policy
- Freedom of Information Public Schedule
- Data Retention Schedule
- Online Safety Policy
- Data Breach Procedure
- Subject Access Request Procedure

2. Roles and responsibilities

This policy applies to all staff employed by Aspire Academies Trust, and to external organisations or individuals working on our behalf.

Staff who do not comply with this policy may face disciplinary action.

Trustee's board

- The trustee's board has overall responsibility for ensuring that our Academies comply with all relevant data protection obligations.

Data protection officer

- The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

- They will provide an annual report of their activities directly to the Trustee board and, where relevant, report to the board their advice and recommendations on Aspire Academies Trust data protection issues.
- The DPO is also the first point of contact for individuals whose data the Aspire Academies Trust processes, and for the ICO.
- Full details of the DPO's responsibilities are set out in the DPO Responsibilities.
- Our DPO is Michelle Fennelly who is contactable via email DPO@aspireacademies.org.uk or phone 07951 359 196.

Data Champions

- The data champions act as the representative of the data controller on a day-to-day basis. Full details of the data champion's responsibilities are set out in the Data Champion Responsibilities.

All staff

Staff are responsible for:

- Collecting, storing, and processing any personal data in accordance with this policy
- Informing the Aspire Academies Trust of any changes to their personal data, such as a change of address.
- Contacting the DPO in the following circumstances:
    1. With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
    2. If they have any concerns that this policy is not being followed
    3. If they are unsure whether they have a lawful basis to use personal data in a particular way
    4. 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 European Economic Area
    5. If there has been a data breach
    6. Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    7. If they need help with any contracts or sharing personal data with third parties

3. Personal Data

'Personal data' is information that identifies an individual and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain. A subset of personal data is known as 'special category personal data'. This special category data is information that relates to:

- Race or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Physical or mental health.
- An individual's sex life or sexual orientation.
- Generic or biometric data for the purpose of uniquely identifying a natural person Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

The Trust does not intend to seek or hold sensitive personal data about staff or pupils except where the Trust has been notified of the information, or it comes to the Trust's attention via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good

practice. Staff or pupils are under no obligation to disclose to the Trust their race or ethnic origin, political or religious beliefs, whether they are a trade union member or details of their sexual life (save to the extent that details of marital status and / or parenthood are needed for other purposes, e.g. pension entitlements).

4. The Data Protection Principles

The GDPR is based on data protection principles that our 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 Trust aims to comply with these principles.

The Trust is committed to always complying with the above principles. This means that the Trust will:

- Inform individuals as to the purpose of collecting any information from them, as and when the Trust ask for it.
- Be responsible for checking the quality and accuracy of the information.
- Regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the data retention policy.
- Ensure that when information is authorised for it is done appropriately.
- Ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system and always follow the relevant security policy requirements.
- Share personal information with others only when it is necessary and legally appropriate to do so.
- Set out clear procedures for responding to requests for access to personal information known as subject access requests.
- Report any breaches of the GDPR in accordance with the procedure in paragraph 9 below.

5. Conditions for processing in the first data protection principle

The Trust will only process personal data where the Trust have one of six 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Aspire Academies Trust can fulfil a contract with the individual, or the individual has asked the Aspire Academies Trust to take specific steps before entering a contract.
- The data needs to be processed so that the Aspire Academies Trust can comply with a legal
- obligation
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life.
- The data needs to be processed so that the Aspire Academies Trust, as a public authority, can perform a task in the public interest, and carry out its official functions.
- The data needs to be processed for the legitimate interests of the Aspire Academies Trust 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.

- When special category personal data is being processed then an additional legal reason must apply to that processing. The Trust will normally only process special category personal data under following legal grounds:
- The processing is necessary for employment law purposes, for example in relation to sickness absence.
- The processing is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment.
- The processing is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities.

Where none of the above apply then the Trust will seek the consent of the data subject to the processing of their special category personal data.

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 personal consent (except for online counselling and preventative services.

6. Use of personal data by the Academy

The Trust holds personal data on pupils, staff and other individuals such as visitors. In each case, the personal data must be treated in accordance with the data protection principles as outlined in paragraph 5 above.

Pupils.

- The personal data held regarding pupils includes contact details, assessment / examination results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information, and photographs.
- The data is used to support the education of the pupils, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how the Trust the academy as a whole is doing, together with any other uses normally associated with this provision in an academy environment.

In particular, the Academy may:

- transfer information to any association society or club set up for the purpose of maintaining contact with pupils or for fundraising, marketing or promotional purposes relating to the academy but only where consent has been obtained first.
- make personal data, including sensitive personal data, available to staff for planning curricular or extra-curricular activities.
- keep the pupil's previous school informed of his / her academic progress and achievements e.g.
- sending a copy of the school reports for the pupil's first year at the academy to their previous school.
- Use photographs of pupils in accordance with the photograph policy.

Any wish to limit or object to any use of personal data should be notified to your Academy Principal in writing, which notice will be acknowledged by the academy in writing. If, in the view of Academy Principal, the objection cannot be maintained, the individual will be given written reasons why the academy cannot comply with their request.

Staff.

- The personal data held about staff will include contact details, employment history, information relating to career progression, information relating to DBS checks, training records, photographs.
- The data is used to comply with legal obligations placed on the Trust in relation to employment, and the education of children in a school environment. The Trust may pass information to other regulatory authorities where appropriate and may use names and photographs of staff in publicity and promotional material. Personal data will also be used when giving references.
- Staff should note that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as "spent" once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.

Any wish to limit or object to the uses to which personal data is to be put should be notified to the Director of Human Resources who will ensure that this is recorded and adhered to if appropriate. If the Director of Human Resources is of the view that it is not appropriate to limit the use of personal data in the way specified, the individual will be given written reasons why the Trust cannot comply with their request.

Other Individuals

The Trust may hold personal information in relation to other individuals who have contact with the academies, such as volunteers and guests. Such information shall be held only in accordance with the data protection principles and shall not be kept longer than necessary.

7. Security of personal data

The Trust 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 Academy off site data register.
- Passwords that are at least eight characters long containing letters and numbers are used to access Aspire Academies Trust computers, laptops, and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals.
- Staff, pupils, or governors who store personal information on their personal devices are expected to follow the same security procedures as for Aspire Academies Trust-owned equipment.
- Where the Trust need to share personal data with a third party, the Trust carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

8. Disclosure of personal data to third parties

The Trust will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk.
- The Trust need to liaise with other agencies – the Trust 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, the Trust will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.

- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data the Trust share.
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

The Trust will also share personal data with law enforcement and government bodies where the Trust are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC.
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided

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

Where the Trust transfer personal data to a country or territory outside the European Economic Area, the Trust will do so in accordance with data protection law.

9. Confidentiality of pupil concerns

Where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or guardian, the academy will maintain confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding their consent, or where the academy believes disclosure will be in the best interests of the pupil or other pupils.

Anybody who makes a request to see any personal information held about them by the Trust is making a subject access request. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure, provided that they constitute a "filing system".

All requests should be sent to the Data Protection Officer and must be dealt with in full without delay and at the latest within one month of receipt. Where a child or young person does not have sufficient understanding to make his or her own request (usually those under the age of 12, or over 12 but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf.

The Data Protection Officer must, however, be satisfied that:

- The child or young person lacks sufficient understanding; and
- The request made on behalf of the child or young person is in their interests.

Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances the academy must have written evidence that the individual has authorised the person to make the application and the Academy

Principal must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

A subject access request must be made in writing. The academy may ask for any further information reasonably required to locate the information.
The academy has 1 month to respond to a Subject Access Request, this can be extended by a further 2 months for complex requests.

An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

All files must be reviewed by the Academy Principal before any disclosure takes place. Access will not be granted before this review has taken place.

Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

10. Exemptions of access to data by subjects

Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived.

There are other exemptions from the right of subject access. If the Trust intend to apply any of them to a request, then the Trust will usually explain which exemption is being applied and why.

11. CCTV
We use CCTV in our academies to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

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 should be directed to the DPO.

12. Photographs, Videos and Audio Recordings
As part of the Aspire Academies Trust's activities, we may take photographs, audio recordings and record images of individuals within our academies.

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

Uses may include:

- Within the academy on notice boards and in academy magazines, brochures, and newsletters etc
- Outside of Aspire Academies Trust by external agencies such as the Aspire Academies Trust photographer, newspapers, campaigns.
- Online on our Aspire Academies Trust 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.

13. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all 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 privacy impact assessments where the Aspire Academies Trust'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.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our Aspire Academies Trust 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, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

14. 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 Aspire Academies Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

15. Subject Access Requests & Other rights of individuals

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Aspire Academies Trust 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 isn't 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.

Subject access requests must be submitted in writing, by letter, email, or fax 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 request the data subject to complete the relevant request form and return it to dpo@aspireacademies.org.uk where they will then receive acknowledgement of receipt and a proposed response date. Staff should also inform the DPO of the initial request.

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 Aspire Academies Trust 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.

Responding to subject access requests

When responding to requests, the Trust:

- Will ask the individual to complete the SAR Request Form and provide 2 forms of identification.
- Will contact the individual via email to confirm the request was made.
- Will respond without delay and within 1 month of receipt of the request.
- Will provide the information free of charge.
- May tell the individual the Trust will comply within 3 months of receipt of the request, where a request is complex or numerous. The Trust will inform the individual of this within 1 month and explain why the extension is necessary.

The Trust will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual.
- Would reveal that the child 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.

If the request is unfounded or excessive, the Trust may refuse to act on it, or charge a reasonable fee, which considers administrative costs.

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

When the Trust refuse a request, the Trust will tell the individual why, and tell them they have the right to complain to the ICO.

Other data protection rights of the individual

In addition to the right to make a subject access request, and to receive information when the Trust are collecting their data about how the Trust use and process it. 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 based on public interest.
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- 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.
- 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.

16. Personal Data Breach

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

In the unlikely event of a suspected data breach, the Trust will follow its data breach procedure.

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

- A non-anonymised dataset being published on the Aspire Academies Trust 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 Aspire Academies Trust laptop containing non-encrypted personal data about pupils.

17. Privacy Impact Assessments (PIAs)

All new projects or policies (including software/technical programmes) containing or collecting personal information will be subject to a Data Privacy Impact Assessment (PIA). All DPIAs should be recorded by the Data Protection Officer.

18. Training

All staff are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Aspire Academies Trust's processes make it necessary.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and updated if necessary, following a change in legislation or guidance. This policy will be ratified by trustees annually.

20. Complaints

Complaints about the above procedures should be made to the DPO at dpo@aspireacademies.org.uk who will decide whether it is appropriate for the complaint to be dealt with in accordance with the academy's complaint procedure.

The Information Commissioner (ICO) can deal with complaints, which are not appropriate to be dealt with through the academy's complaint procedure. Contact details of both will be provided with the disclosure information.

FREEDOM OF INFORMATION:

1. Introduction

The Trust is subject to the Freedom of Information Act 2000 (FOI) as a public authority, and as such, must comply with any requests for information in accordance with the principles laid out in the Act.

2. What is a request under FOI?

Any request for any information from the Trust is technically a request under the FOI, whether the individual making the request mentions the FOI. However, the ICO has stated that routine requests for information (such as a parent requesting a copy of a policy) can be dealt with outside of the provisions of the Act.

All requests should be referred in the first instance to the Data Protection Officer, who may allocate another individual to deal with the request. This must be done promptly, and in any event within 3 working days of receiving the request.

When considering a request under FOI, you must bear in mind that release under FOI is treated as release to the public, and so once it has been released to an individual, anyone can then access it, and you cannot restrict access when releasing by marking the information "confidential" or "restricted".

3. Time limit for compliance

The Trust must respond as soon as possible, and in any event, within 20 working days of the date of receipt of the request. For an Academy when calculating the 20-working day deadline, a "working day" is a school day (one in which pupils are in attendance), subject to an absolute maximum of 60 normal working days (not school days) to respond.

4. Procedure for dealing with a request.

All requests should be referred in the first instance to the Data Protection Officer, who may reallocate to an individual with responsibility for the type of information requested.

The first stage in responding is to determine whether the Trust "holds" the information requested. The Trust will hold the information if it exists in computer or paper format. Some requests will require the Trust to take information from different sources and manipulate it in some way. Where this would take minimal effort, the Trust is considered to "hold" that information, but if the required manipulation would take a significant amount of time, the requestor should be contacted to explain that the information is not held in the manner requested and offered the opportunity to refine their request. For example, if a request required the Trust to add up totals in a spreadsheet and release the total figures, this would be information "held" by the Trust. If the Trust would have to go through several spreadsheets and identify individual figures and provide a total, this is likely not to be information "held" by the Trust, depending on the time involved in extracting the information.

The second stage is to decide whether the information can be released, or whether one of the exemptions set out in the Act applies to the information. Common exemptions that might apply include:

- Section 40 (1) – the request is for the applicant's personal data. This must be dealt with under the subject access regime in the DPA, detailed in the DPA policy above.
- Section 40 (2) – compliance with the request would involve releasing third party personal data, and this would be in breach of the DPA principles as set out in paragraph 3.1 of the DPA policy above.
- Section 41 – information that has been sent to the Academy (but not the Academy's own
- information) which is confidential.
- Section 21 – information that is already publicly available, even if payment of a fee is required to access that information.
- Section 22 – information that the Academy intends to publish at a future date.
- Section 43 – information that would prejudice the commercial interests of the Academy and / or a third party.
- Section 38 – information that could prejudice the physical health, mental health or safety of an individual (this may apply particularly to safeguarding information);
- Section 31 – information which may prejudice the effective detection and prevention of crime – such as the location of CCTV cameras.
- Section 36 – information which, in the opinion of the chair of governors of the Academy, would prejudice the effective conduct of the Academy. There is a special form for this on the ICO's the site to assist with the obtaining of the chair's opinion.

The sections mentioned in italics are qualified exemptions. This means that even if the exemption applies to the information, you also must carry out a public interest weighting exercise, balancing the public interest in the information being released, as against the public interest in withholding the information.

5. Responding to a request

When responding to a request where the Trust has withheld some or all the information, the Trust must explain why the information has been withheld, quoting the appropriate section number and explaining how the information requested fits within that exemption. If the public interest test has been applied, this also needs to be explained.

The letter should end by explaining to the requestor how they can complain – either by reference to an internal review by a governor, or by writing to the ICO.

6. Dealing with Vexatious or Repeated Requests

Should an applicant make a 'vexatious' or 'repeated' request for identical or substantially similar information, the academy/trust will inform the applicant in writing that they will not fulfil the request. When responding in this manner the Trust will offer assistance to the individual, by indicating why they consider the request is vexatious or repeated.

7. Contact

Any questions about this policy should be directed in the first instance to the Data Protection Officer.

FREEDOM OF INFORMATION PUBLICATION SCHEDULE:

Information to be published	**How the information can be obtained**
Class 1 - Who we are and what we do	
Instrument of Government The Instrument of Government is the document which records the name and category of the academy and the name and constitution of its governing body.	Academy website or www.AspireAcacdemies.org.uk
Academy prospectus The statutory contents of the Academy prospectus, as follows: - information about the implementation of the governing body's policy on pupils with special educational needs (SEN). - a description of the policies relating to disabled pupils, including facilities to improve access and the accessibility plan. Once the prospectus has been published and made available to parents, access to it should be available to anyone.	Academy website. Hard copy on request.
Advisory Body and Board of Trustees The names, and contact details of the governors should be available and the basis on which they have been appointed.	Academy website or www.AspireAcacdemies.org.uk
School session times and term dates Details of school session times and dates of school terms and holidays.	Academy website.
Location and contact information The address, telephone number and website for the school together with the names of key personnel.	Academy website or www.AspireAcacdemies.org.uk
Class 2 - What we spend and how we spend it	
Annual budget plan and financial statements Details of the Individual Schools Budget distributed by the Local Authority and the school's annual income and expenditure returns.	Academy website or www.AspireAcacdemies.org.uk
Capital funding Details of the capital funding allocated to the school together with information on related building projects and other capital projects.	Academy website or www.AspireAcacdemies.org.uk
Additional Funding	Academy website or www.AspireAcacdemies.org.uk

Income generation schemes and other sources of funding. (Specialist secondary schools may have additional government funding and arrangements with private sector sponsors.)	
Procurement and contracts Details of procedures used for the acquisition of goods and services. Details of contracts that have gone through a formal tendering process.	Academy website or www.AspireAcacdemies.org.uk
Pay policy The statement of the school's policy and procedures regarding teachers' pay.	Academy website or www.AspireAcacdemies.org.uk
Staffing and grading structure	Academy website or www.AspireAcacdemies.org.uk
Governors' allowances Details of allowances and expenses that can be claimed or incurred.	Academy website or www.AspireAcacdemies.org.uk
Class 3 - What our priorities are and how we are doing	
School profile Government-supplied performance data	Academy website
Summary of latest Ofsted report* The required narrative sections covering areas such as: successes during the year; areas of improvement; efforts to meet the individual needs of every child; pupil's health, safety and support; post-Ofsted action plan; and links with parents and the community. *the full Ofsted report should also be available.	Academy website or http://reports.ofsted.gov.uk
Performance management information Performance management policy and procedures adopted by the advisory body.	Academy website or www.AspireAcacdemies.org.uk
School's future plans Any major proposals for the future of the school involving, for example, consultation or a change in school status.	Academy website or www.AspireAcacdemies.org.uk
Every Child Matters / child protection The contribution of the school to the five Every Child Matters outcomes. The policies and procedures that are in place to ensure that functions are exercised with a view to safeguarding and promoting the welfare of children in compliance with any guidance issued by the Secretary of State	Academy website or www.AspireAcacdemies.org.uk

Class 4 - How we make decisions	
Admissions policy / decisions The school's admission arrangements and procedures, together with information about the right of appeal. Individual admission decisions would not be expected to be published, but information on application numbers/patterns of successful applicants (including criteria on which applications were successful) should be if this information is held by the school.	Academy website
Minutes of meetings of the Advisory body and its subcommittees Minutes, agendas and papers considered at such meetings are available on request, with the exception of information that is properly considered to be private to the meeting.	Hard copy on request
Class 5 - Our policies and procedures	
School policies This will include school policies and procedures together with other information related to the school such as charging and remissions policy, health and safety and risk assessment, complaints procedure, staff conduct policy, discipline and grievance policies, pay policy, staffing structure implementation plan. It will also include policies and procedures for handling information requests.	Academy website or www.AspireAcacdemies.org.uk
Pupil and Curriculum policies This will include such policies as home-school agreement, curriculum, sex education, special educational needs, accessibility, race equality, collective worship, careers education (Key Stage 4 pupils) and pupil discipline.	Academy website
Records management and personal data policies This will include information security policies, records retention, destruction and archive policies, and data protection (including data sharing) policies.	Academy website or www.AspireAcacdemies.org.uk
Equality and diversity This will also include policies, schemes, statements, procedures and guidelines relating to equal opportunities.	Academy website or www.AspireAcacdemies.org.uk
Policies and procedures for the recruitment of staff If vacancies are advertised as part of recruitment policies, details of current vacancies will be readily available.	Academy website or www.AspireAcacdemies.org.uk
Charging regimes and policies Details of any statutory charging regimes should be provided. Charging policies should include charges made for information	Academy website or

routinely published. They should clearly state what costs are to be recovered, the basis on which they are made, and how they are calculated.	www.AspireAcacdemies.org.uk
Class 6 - Lists and registers	
Curriculum circulars and statutory instruments Statutory Instruments (for example Regulations), departmental circulars and administrative memoranda sent to the Head Teacher/Governing Body concerning the curriculum.	Academy website
Disclosure logs If a school produces a disclosure log indicating the information provided in response to requests, it should be readily available. Disclosure logs are recommended as good practice.	N/A
Asset register We would expect some information from capital asset registers to be available if such registers are held.	Included in Aspire Academies Trust financial statement.
Any information the school is currently legally required to hold in publicly available registers.	Academy website
The services we offer	
Generally, this is an extension of part of the first class of information and may also relate to information covered in other classes. Examples of services that could be included here are: - Extra-curricular activities - Out of school clubs - School publications	Academy website
Services for which the school is entitled to recover a fee, together with those fees	Academy website
Leaflets, booklets, and newsletters.	Academy website

Appendix 1

Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO via email at DPO@aspireacademies.org.uk
- 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 Principal and the Board of Trustees.

The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out 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.
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material, or nonmaterial damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud.
    - Financial loss.
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned.

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- 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. Documented decisions are stored on the Bovingdon Z: drive, under GDPR Compliance.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. 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 o 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. 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.
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach o 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 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 o 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 on the Bovingdon Z: drive, under GDPR Compliance.

The DPO and Principal will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches.

We will take the actions set out below 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.

Email Breaches:

- 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 DPO as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it.
- In any cases where the recall is unsuccessful, the DPO will 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 DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
- The 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.

Lost / stolen devices.

- If a Trust laptop is lost/stolen the DPO will require the staff member to confirm that no personal data was saved on the device (There should not be any personal data saved on the device as per our data protection policy
- If a Trust mobile phone is lost / stolen, the DPO will contact the phone provider who will disable the device. The DPO will also contact the IT provider who will disable email account on this device. (You must be using outlook app as per our data protection policy)
- If a Trust IPAD is lost/stolen the DPO will contact the IT provider who will wipe the device using MDM.
- If a personal device is lost (If Aspire Academies Trust emails are on the device), the staff member must contact their phone provider who will disable the device. The DPO will then contact the IT provider who will disable the email account (You must be using outlook app as per our data protection policy) Unauthorized account access:
- If a staff member's email account has unauthorized access, they must inform the DPO who will contact the IT provider, they will investigate using the access log and will change the password on the account to prevent further breaches.
- If a staff members computer log in has unauthorized access the DPO will contact the IT provider who will investigate and change password on the account to prevent further breaches.

Appendix 2:

Responding to subject access requests made under GDPR.

1. Rights of access to information

Individuals have a right to make a 'subject access request' to gain access to personal information that the Aspire Academies Trust 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 isn't 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.

2. Managing a subject access request

Subject access requests must be submitted in writing, by either letter, email, or fax 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.

When responding to requests, we:

- Will ask the data subject to complete the SAR Request Form and to provide 2 forms of identification.
- Will contact the individual in writing to acknowledge receipt of the request and to outline the proposed response date.
- Will respond without delay and within 30 days of receipt of the request.
- Will provide the information free of charge (innless the request is 'Unfounded or excessive')
- 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 will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual.
- Would reveal that the child 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.

3. **Unfounded or Excessive requests.**
   If the request is unfounded or excessive, you can either:

   - Charge a reasonable fee for you to comply, based on the administrative cost of providing the information.
   - Refuse to respond.
   - Comply within 3 months, rather than the usual deadline of 1 month - you must inform the individual of this and will explain why.

   'Unfounded or excessive' means that the request is repetitive or asks for further copies of the same information.

4. **Refusing a request.**
   When you refuse a request, you must:

   - Respond to them within 1 month.
   - Explain why you are refusing the requests.
   - Tell the individual they have the right to complain to the ICO.

5. **Redaction**
   Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained to establish, if a complaint is made, what was redacted and why.

6. **Complaints**
   Complaints about the above procedures should be made to the DPO who will decide whether it is appropriate for the complaint to be dealt with in accordance with the academy's complaint procedure.

   Complaints which are not appropriate to be dealt with through the academy's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Appendix 3

DPO Responsibilities

The key responsibility of the DPO is to ensure compliance with GDPR by:

- Advising the Trust and its employees of their obligations under relevant data protection law, including the GDPR
- Monitoring compliance with data protection law, by: Collecting information to identify data processing activities.
- Analysing and checking the compliance of data processing activities
- Informing, advising, and issuing recommendations to the school
- Ensuring the school's policies are followed within the school, by:
- Assigning responsibilities to staff members
- Raising awareness of data protection law, including the GDPR, across the school
- Supporting staff with queries
- Conducting internal audits
- DPOs will advise Academies of their obligations under data protection law.
- Advise on and assist the Academies with carrying out data protection impact assessments, if necessary
- Act as a contact point for the ICO (as the 'supervisory authority'), involving:
- Helping the ICO to access documents and information.
- Seeking advice on data protection issues
- Act as a contact point for individuals whose data is processed (staff, pupils, and parents, for example)
- Take a risk-based approach to data protection, involving:
- Prioritising the higher-risk areas of data protection and focusing on these the most
- Using their common sense to advise the school on whether it should conduct an audit, provide training in certain areas, and determine what the DPO should spend the most time doing.

Appendix 4

Data Champions Responsibilities

The key responsibility of the Data champion is:

- To be the first point of contact for GDPR questions.
- To escalate difficult questions to the Data Protection 0fficer.
- To coordinate searches for subject access request data.
- To coordinate searches in response to requests to be forgotten.
- To act as a channel of communication between the Data Protection Officer and their Academy.
- Update the information asset register & consent registers for their academy.
- Carry out data impact assessments with the Data Protection Officer when requesting new special category data.