ASCENT ACADEMIES' TRUST

DATA PROTECTION (GDPR) POLICY

Policy reviewed and approved by Trustees	**October 2022**
Version	**v3.0**
Review frequency	**2 years**
Date of next review	**October 2024**
Responsible Officer	**Chief Operating Officer**

Contents

Data Protection (GDPR) Policy

1. AIMS

The Ascent Academies' Trust aims to ensure that all personal data collected about staff, pupils, parents, trustees, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

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 GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

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

In addition, this policy complies with the Trust's 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.

4. THE DATA CONTROLLER

The Trust processes personal data relating to parents, pupils, staff, trustees, visitors and others, and therefore is a data controller.

The Ascent Academies' Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. ROLES AND RESPONSIBILITIES

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

5.1 Board of Trustees

The Board of Trustees has overall responsibility for ensuring that the Trust complies with all relevant data protection obligations.

5.2 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, where relevant, report to the board their advice and recommendations on Trust data protection issues.

The DPO is also the first point of contact for individuals whose data the Trust processes, and for the ICO. The DPO will work closely with the Trust Business Manager (TBM) and Trust Strategic IT Manager (ITM) on operational matters within the Trust.

Full details of the DPO's responsibilities are set out in their job description. The Trust's DPO is Nick Humphreys and is contactable via email (data.protection@sunderland.gov.uk) or by phone (07769 672633).

5.3 Executive Leadership Team/ Heads of Academy
The Executive Leaders and Heads of Academy act as the representatives 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 Trust of any changes to their personal data, such as a change of address
- Contacting the TBM/ITM in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - 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 European Economic Area
    - 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 GDPR is based on data protection principles that the Trust 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 the Trust aims to comply with these principles.

7. COLLECTING PERSONAL DATA

7.1 Lawfulness, fairness and transparency

The Trust will only process personal data where it has one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Trust can **fulfil a contract** with the individual, or the individual has asked the Trust to take specific steps before entering into a contract
- The data needs to be processed so that the 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 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 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**

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

If the Trust offer online services to pupils, such as classroom apps, and it intends to rely on consent as a basis for processing, it will get parental consent where the pupil is under 13 (except for online counselling and preventive services) or where pupils over that age do not have the required level of understanding due to their special educational needs.

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

7.2 Limitation, minimisation and accuracy

The Trust will only collect personal data for specified, explicit and legitimate reasons. It will explain these reasons to the individuals when it first collects their data.

If the Trust wishes to use personal data for reasons other than those given when the data was first obtained the Trust will inform the individuals concerned before it does so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. 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 Trust's record retention schedule.

8. SHARING PERSONAL DATA

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 staff at risk
- It needs to liaise with other agencies – it will seek consent as necessary before doing this
- It's suppliers or contractors need data to enable the Trust to provide services to 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 shared
- Only share data that the supplier or contractor needs to carry out their service and information necessary to keep them safe while working with the Trust

The Trust will also share personal data with law enforcement and government bodies where it is legally required to do so including:

- 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 the Trust's safeguarding obligations
- Research and statistical purposes, providing 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 situation that affects pupils or staff.

Where the Trust transfers personal data to a country or territory outside the European Economic Area, it will do so in accordance with 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 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 can be submitted verbally or in writing, either by letter, email or fax to the Trust. Requests 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 their Head of Academy, who will liaise with the TBM.

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 aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from parents or carers of pupils within the Trust may not be granted without the express permission of the pupil unless the child is under this age. 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, the Trust:

- 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
- Will provide the information free of charge
- May tell the individual it 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 may 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
- Is subject to an applicable exemption under Schedules 2 to 4 of the Data Protection Act 2018

If the request is complex or excessive, the Trust may extend the deadline for response by two calendar months, refuse to act on it, or charge a reasonable fee which takes into account 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 refuses a request, it will tell the individual why, and tell them they have the right to complain to the ICO.

Staff may request access to personnel information held about them in their personnel file. The request must be submitted in advance and an arrangement will be made for them to view their file. The right is for them to access the information and the personnel file cannot be removed. The request should be submitted to their Head of Academy or the Chief Operating Officer

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 the Trust is collecting their data about how it is used and processed (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask the Trust 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 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 their Head of Academy. If staff receive such a request, they must immediately forward it to their Head of Academy.

10. PARENTAL REQUESTS TO SEE THE EDUCATIONAL RECORD

There is no automatic right for parents, or those with parental responsibility, to have access to their child's educational record (which includes most information about a pupil). However, the Trust will endeavour to provide this information and requests should be made following the procedures outlined in Section 9.

11. CCTV

The Trust uses CCTV in various locations around Trust sites to ensure they remain safe.

The Trust will adhere to the ICO's code of practice for the use of CCTV.

The Trust do not need to ask individuals' permission to use CCTV, but it 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 to Mr D Orton, Assets and Estates Manager.

12. PHOTOGRAPHS AND VIDEOS

As part of Trust activities, staff may take photographs and record images of individuals within academies.

The Trust will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where there is a need for parental consent, the Trust will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where there isn't a need for parental consent, the Trust will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

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

Consent can be refused or withdrawn at any time. If consent is withdrawn, the Trust will delete the photographs or videos and not distribute them further.

When using photographs and videos in this way the Trust will not accompany them with personal information about the child, to reduce the risk of identification..

More information on the use of photographs and videos can be found in the individual academies' child protection policies and safeguarding adults' policies.

13. DATA PROTECTION BY DESIGN AND DEFAULT

The Trust will put measures in place to show that it has integrated data protection into all of its 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 (DPIAs) where the 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, ensuring a record of attendance is maintained
- Regularly conducting reviews and audits to test privacy measures and make sure the Trust is compliant
- Maintaining records of processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of individual academies and DPO and all information the Trust is required to share about the use and processing of their personal data (via privacy notices)
    - For all personal data held, maintaining an internal record of the type of data, data subject, how and why the data is used, any third-party recipients, how and why the data is stored, retention periods and how the data secure is kept secure

14. DATA SECURITY AND STORAGE OF RECORDS

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 via one of the individual academy offices
- Secure passwords are used to access Trust computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- The use of USB devices and external hard drives is not permitted
- Staff, pupils or trustees are not permitted to store personal information on their personal devices
- The ability to save data onto local drives (eg C drive) is restricted
- 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)

15. 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 the Trust cannot or do not need to rectify or update it.

For example, the Trust will shred or incinerate paper-based records, and overwrite or delete electronic files. The Trust may also use a third party to safely dispose of records on its behalf. If it does so, the Trust will require the third party to provide sufficient guarantees that it complies with data protection law and WEE guidelines.

16. PERSONAL DATA BREACHES

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 the procedure set out in Appendix 1.

When appropriate, the Trust 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 academy website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person

17. TRAINING

All staff and trustees 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 Trust's processes make it necessary.

18. MONITORING ARRANGEMENTS

The Chief Operating Officer is responsible for monitoring and reviewing this policy, in conjunction with the DPO. This policy will be reviewed **every 2 years** and shared with the Board of Trustees.

19. LINKS WITH OTHER POLICIES

This data protection policy is linked to our:

- Freedom of information publication scheme
- Individual academies' Child Protection Policies
- For applicable individual academies, their Safeguarding Adults Policies
- IT Acceptable Use policy
- Social Media Policy
- Online Safety Policy

APPENDIX 1

Personal 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 their Head of Academy and the Trust Business Manager
- The HOA will investigate the report and determine whether a breach has occurred. The HOA 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 HOA will report findings to the TBM

- The TBM will alert the DPO and nominated Trustee
- The Trust 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 TBM, in conjunction with 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. The DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material 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 Trust's network.
- 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

    - 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
    - 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 TBM 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 on the Trust's network.
- The TBM and Head of Academy will review what happened and how it can be stopped from happening again. This discussion will occur as soon as reasonably possible

Actions to minimise the impact of data breaches

The Trust 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. The Trust will review the effectiveness of these actions and amend them as necessary after any data breach.

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 HOA/TBM as soon as they become aware of the error*
- *If the sender is unavailable or cannot recall the email for any reason, the HOA will ask the ICT department to recall it*
- *In any cases where the recall is unsuccessful, the HOA 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 HOA will ensure the Trust receives a written response from all the individuals who received the data, confirming that they have complied with this request*
- *The HOA will carry out an internet search to check that the information has not been made public; if it has, the Trust will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*

Other types of breach to consider could include:

- *Details of pupil premium interventions for named children being published on academy website*
- *Non-anonymised pupil exam results being shared with trustees*