Aletheia Academies Trust

GDPR and Data Protection Policy

April 2022

Company Number:	07801612
Approved By:	Board of Trustees
Policy Type:	Statutory
Adopted on:	April 2022
Date of Next Review:	April 2024
Review Period:	2 years

GDPR and Data Protection Policy for Schools

General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA) is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

This policy is intended to ensure personal information is dealt with properly and securely in accordance with the legislation. It will apply to personal information regardless of how it is used, recorded, stored, and whether it is held in paper files or electronically.

Policy Objectives

The Trust as the Data Controller will comply with its obligations under the GDPR and the DPA. The Trust is committed to being clear and transparent about how it obtains and processes personal information and will ensure data subjects are aware of their rights under the legislation.

All staff must have a general understanding of the law and understand how it may affect their decisions to make an informed judgement about how information is gathered, used, and ultimately deleted. All staff must read, understand, and comply with this policy.

The Information Commissioner as the Regulator can impose fines of up to 20 million Euros (approximately £17 million) for serious breaches of the GDPR, therefore it is imperative the Trust and all staff comply with the legislation.

Scope of the Policy

Personal data is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information. The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under the GDPR, personal information also includes an identifier such as a name, an identification number (including online), or location data.

The Trust collects a large amount of personal data every year including pupil records, staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by the Trust. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies, and other bodies.

The Principles

The principles set out in the GDPR must be adhered to when processing personal data:

1. Personal data must be processed lawfully, fairly and in a transparent manner (lawfulness, fairness, and transparency).
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation).
3. Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purpose(s) for which they are processed (data minimisation).
4. Personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay (accuracy).
5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed (storage limitation).
6. Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal information is processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data (integrity and confidentiality).

Transfer Limitation

Personal data shall not be transferred to a country outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data as determined by the European Commission or where the organisation receiving the data has provided adequate safeguards.

Data may be transferred where the data subject has provided explicit consent or for other limited reasons. Staff should contact the DPO if they require further assistance with a proposed transfer of personal data outside of the EEA.

Lawful Basis for Processing Personal Information

Before any processing activity starts for the first time and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be carefully selected to demonstrate compliance with the data protection principles and include information about both the purposes of the processing and the lawful basis for it in the Trust's relevant privacy notice(s).

(a) The data subject has given consent to the processing of his or her data for one or more specific purposes.
(b) Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract.
(c) Processing is necessary for compliance with a legal obligation to which the data controller is subject.
(d) Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
(e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Trust.
(f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. (The first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks).

Consent

Agreement must be indicated clearly either by a statement or positive action to the processing. Consent requires affirmative action, so silence, pre-ticked boxes, or inactivity are unlikely to be enough. If consent is given in a document which deals with other distinct matters, the consent must be kept separate.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be reviewed if personal data is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first gave consent.

Sensitive Personal Information

Processing of sensitive personal information (known as 'special categories of personal data') is prohibited unless a lawful special condition for processing is identified.

Sensitive personal information is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person.

Sensitive personal information will only be processed if:

- There is a lawful basis for doing so as identified previously
- One of the special conditions for processing sensitive personal information applies:

(a) The individual ('data subject') has given explicit consent (which has been clearly explained in a privacy notice).
(b) The processing is necessary for the purposes of exercising the employment law rights or obligations of the Trust or the data subject.
(c) The processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent.
(d) The processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim.
(e) The processing relates to personal data which are manifestly made public by the data subject.
(f) The processing is necessary for the establishment, exercise, or defence of legal claims.
(g) The processing is necessary for reasons of substantial public interest.
(h) The processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services.
(i) The processing is necessary for reasons of public interest in the area of public health.

The Trust's privacy notice(s) set out the types of sensitive personal information that it processes, what it is used for, the lawful basis for the processing, and the special condition that applies.

Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out, and the legal basis for it.

Unless the Trust can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data. Evidence of consent will need to be captured and recorded so that the Trust can demonstrate compliance with the GDPR.

Automated Decision Making

Where the Trust carries out automated decision making (including profiling) it must meet all the principles and have a lawful basis for the processing. Explicit consent will usually be required for automated decision making (unless it is authorised by law, or it is necessary for the performance of entering into a contract).

Additional safeguards and restrictions apply in the case of solely automated decision-making, including profiling. The Trust must notify the data subject as soon as reasonably possible in writing, that a decision has been taken based on solely automated processing and that the data subject may request the Trust to reconsider or take a new decision. If such a request is received, the Trust must reply within 21 days.

Data Protection Impact Assessments (DPIA)

All data controllers are required to implement 'privacy by design' when processing personal data.

This means the Trust's processes must embed privacy considerations and incorporate appropriate technical and organisational measures in an effective manner to ensure compliance with data privacy principles.

Where processing is likely to result in high risk to an individual's data protection rights (e.g., where a new technology is being implemented) a DPIA must be carried out to assess:

- The risks to individuals
- What measures can be put in place to address those risks and protect personal information
- Whether the processing is necessary and proportionate in relation to its purpose

Documentation and Records

Written records of processing activities must be kept and recorded including:

- A description of the categories of individuals and categories of personal data
- A description of technical and organisational security measures
- Categories of recipients of personal data
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place
- Retention schedules
- The name(s) and details of individuals or roles that carry out the processing
- The purposes of the processing

As part of the Trust's record of processing activities the DPO will document, or link to documentation, where accessible, on:

- Information required for privacy notices
- Location(s) of personal information
- Records of consent
- Records of data breaches

Records of processing of sensitive information are kept on:

- Relevant purposes for which the processing takes place, including why it is necessary for that purpose
- The lawful basis for our processing
- Whether the personal information is retained or erased in accordance with the retention schedule and, if not, the reasons for not following the policy

The Trust should conduct regular reviews of the personal information it processes and update its documentation accordingly. This may include:

- Carrying out information audits to find out what personal information is held
- Reviewing policies, procedures, contracts, and agreements to address retention, and security and data sharing
- Talking to staff about their processing activities

Privacy Notice

The Trust will issue privacy notices as required, informing data subjects (or their parents, depending on age of the pupil) about the personal information that it collects and holds relating to individual data subjects, how individuals can expect their personal information to be used and for what purposes.

When information is collected directly from data subjects, including for HR or employment purposes, the data subject shall be given all the information required by the GDPR including how and why the Trust will use, process, disclose, protect, and retain that personal data through a privacy notice.

The Trust will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

The Trust will issue a minimum of two privacy notices, one for pupil information, and one for workforce information, and these will be reviewed in line with any statutory or contractual changes.

Purpose Limitation

Personal data must be collected only for specified, explicit, and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

Personal data must not be used for new, different, or incompatible purposes from that disclosed when it was first obtained unless the data subject has been informed of the new purposes and they have consented where necessary.

Data Minimisation

Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

Staff may only process data when their role requires it. Staff must not process personal data for any reason unrelated to their role.

The Trust maintains a retention schedule to ensure personal data is deleted after a reasonable time for the purpose for which it was being held unless a law requires such data to be kept for a minimum time. Staff must take all reasonable steps to destroy or delete all personal data that is held in its systems when it is no longer required in accordance with the schedule. This includes requiring third parties to delete such data where applicable.

Staff must ensure that data subjects are informed of the period for which data is stored and how that period is determined in any applicable privacy notice.

Photographic / Video Use

Photographs or video recordings of children taken by staff, or a contracted 3rd party are often used on display around the Trust, in the Trust prospectus, school produced printed publications, Trust events, or the Trust website. A Trust may also be visited by the media who will take photographs or video recordings of a visiting dignitary or other high-profile event. Children will often appear in these photographs, which may appear in local or national newspapers, or on televised news programmes.

Individual photographic and video consent is gathered upon joining the Trust. Consent can be subsequently changed by contacting the Trust concerned and will apply onwards from date of request.

To safeguard and protect privacy, the Trust prohibits members of the public (including parents) from taking photographs or video recordings during Trust events. Where appropriate for an event, a dedicated photo zone may be earmarked to provide an area where parents may take photographs of their children either alone or within a small group (provided all have given consent).

Individual Rights

Staff as well as any other data subjects have the following rights in relation to their personal information:

- To be informed about how, why, and on what basis that information is processed
- To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request
- To have data corrected if it is inaccurate or incomplete
- To have data erased if it is no longer necessary for the purpose for which it was originally collected and processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten')
- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased) or where the Trust no longer needs the personal information, but you require the data to establish, exercise or defend a legal claim
- To restrict the processing of personal information temporarily where you do not think it is accurate (and the Trust are verifying whether it is accurate), or where you have objected to the processing (and the Trust are considering whether the Trust's legitimate grounds override your interests)
- In limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used, and machine-readable format
- To withdraw consent to processing at any time (if applicable)
- To request a copy of an agreement under which personal data is transferred outside of the EEA
- To object to decisions based solely on automated processing, including profiling
- To be notified of a data breach which is likely to result in high risk to their rights and obligations
- To make a complaint to the ICO or a Court

Individual Responsibilities

During their employment, staff may have access to the personal information of other members of staff, suppliers, clients, or the public. The Trust expects staff to help meet its data protection obligations to those individuals.

If you have access to personal information, you must:

- Only access the personal information that you have authority to access and only for authorised purposes
- Only allow other staff to access personal information if they have appropriate authorisation
- Only allow individuals who are not Trust staff to access personal information if you have specific authority to do so
- Keep personal information secure (e.g., by complying with rules on access to premises, computer access, encryption, password protection, and secure file storage and destruction in accordance with the Trust's policies)
- Not store personal information on local drives or on personal devices that are used for work purposes

The Code of Conduct outlines expected professional responsibilities in detail.

Information Security

The Trust will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

All staff are responsible for keeping information secure in accordance with the legislation and must follow the Trust acceptable usage policies.

The Trust will develop, implement, and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly evaluate the effectiveness of safeguards to ensure security of processing.

Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

Staff must follow all procedures and technologies put in place to maintain the security of all data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and and who agree to put adequate measures in place, as requested.

Staff must maintain data security by protecting the confidentiality, integrity, and availability of the personal data.

Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

Availability means that authorised users can access the personal data when they need it for authorised purposes.

Staff must comply with and not attempt to circumvent the administrative, physical, and technical safeguards the Trust has implemented and maintains in accordance with the GDPR and the DPA.

Where the Trust uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

- The organisation may only act on the written instructions of the Trust
- Those processing data are subject to the duty of confidence
- Appropriate measures are taken to ensure the security of processing
- Sub-contractors are only engaged with the prior consent of the Trust and under a written contract
- The organisation will assist the Trust in providing subject access and allowing individuals to exercise their rights in relation to data protection
- The organisation will delete or return all personal information to the Trust as requested at the end of the contract
- The organisation will submit to audits and inspections, provide the Trust with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the Trust immediately if it does something infringing data protection law

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the DPO.

Storage and Retention of Personal Information

Personal data will be kept securely in accordance with the Trust's data protection obligations.

Personal data should not be retained for any longer than necessary. The length of time data should be retained will depend upon the circumstances, including the reasons why personal data was obtained.

Personal information that is no longer required will be deleted in accordance with retention schedules.

Data Breaches

A data breach may take many different forms:

- Blagging offences where information is obtained by deceiving the holding organisation
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams
- Human error, such as accidental deletion or alteration of data
- Environmental circumstances, such as a fire or flood
- Loss of data resulting from an equipment or systems (including hardware or software) failure
- Loss or theft of data or equipment on which personal information is stored
- Unauthorised access to or use of personal information either by a member of staff or third party

Depending on the severity of a data breach and the likelihood it would result in a high risk to the rights and freedoms of individuals, the Trust may be obligated to report a data breach to the Information Commissioner's Office (ICO) without undue delay, and where possible, within 72 hours.

Staff must inform their line manager, headteacher, or the DPO directly on immediate discovery of a data breach and make all reasonable efforts to secure the data breach and recover any personal information.

Subject Access Requests (SAR)

Anyone can raise a SAR with the Trust to seek personal copies of their personal information. A request should be made in writing to the DPO or headteacher at the relevant school. A SAR request can also be made verbally.

The Trust will take steps to verify the identity of the individual making the SAR request. If any documentation is requested as proof of identify, then the set timescale for responding will not begin until the Trust has received the requested information.

A SAR will be actioned and executed within one calendar month from the date the request was received. The Trust reserves the right to extend this by a further two months if the request is complex, or multiple requests have been received from the individual. To minimise any delays, the Trust encourages a SAR to be focused and targeted in data scope.

In most cases, a fee will not be levied, unless the request is manifestly unfounded or manifestly excessive, or if a request is made for further copies of the data.

The principle of data minimisation will be adopted throughout the searching, gathering, and collation of the SAR. Any personal data that does not pertain to the individual will be redacted to protect the rights of other data subjects. In most cases, the Trust is not required to seek consent from employees wherein their personal data extends into a pending SAR through their professional capacity; providing the employee meets the 'education data test' as defined below.

An education worker meets the 'education data test' if the other individual is:

- an employee of a local authority that maintains a school in England or Wales
- a teacher or other employee at a voluntary aided, foundation or foundation special school, an Academy school, an alternate provision Academy, an independent school or a non-maintained special school in England or Wales
- a teacher at a school in Northern Ireland
- an employee of the Education Authority in Northern Ireland
- an employee of the Council for Catholic Maintained Schools in Northern Ireland
- an employee at an education authority in Scotland (as defined by the Education (Scotland) Act 1980) in connection with their statutory education functions, and the information relates to, or was supplied by the other individual in their capacity as an employee of an education authority

If exemptions apply, the Trust may refuse to provide all or some of the information requested, which may include the entire SAR itself. A SAR may also be refused if the request is manifestly unfounded or manifestly excessive. In such cases, the Trust will inform the individual of:

- The reasons why the SAR request is refused
- Their right to make a complaint to the ICO or another supervisory authority
- Their ability to seek to enforce this right through the courts

A trackable and signed form of postal service will be used to ensure non-repudiation of the SAR package. Any residual files (paper or digital) will be securely destroyed once confirmation of the SAR delivery has been established.

Legal Advice

At any time, the Trust reserves the right to seek qualified legal advice on any aspect of data protection and GDPR through a registered law firm.

Training

The Trust will ensure that staff are adequately trained regarding their data protection responsibilities.

Failure to Comply

The Trust takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and the Trust may in some circumstances amount to a criminal offence by the individual.

Any failure to comply with any part of this policy may lead to disciplinary action under the Trust's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about this policy, you should contact your line manager, headteacher or the DPO.

Review of Policy

This policy will be updated as necessary to reflect best practice or amendments made to the GDPR or the DPA.

The Supervisory Authority in the UK

Please follow this link to the ICO's website (https://ico.org.uk/) which provides detailed guidance on a range of topics including individual's rights, data breaches, dealing with subject access requests, and how to handle requests from third parties for personal data etc.

Glossary

Automated Decision-Making (ADM): when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. GDPR prohibits automated decision-making (unless certain conditions are met), but not automated processing.

Automated Processing: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements. Profiling is an example of automated processing.

Consent: agreement which must be freely given, specific, informed, and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, which signifies agreement to the processing of personal data relating to them.

Data Controller: the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. It is responsible for establishing practices and policies in line with the GDPR. are the Data Controller of all personal data relating to its pupils, parents, and staff.

Data Subject: a living, identified, or identifiable individual about whom we hold personal data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of 'privacy bydesign' and should be conducted for all major systems or business change programs involving the processing of personal data.

Data Protection Officer (DPO): the person required to be appointed in public authorities under the GDPR.

European Economic Area (EEA): the 28 countries in the EU, and Iceland, Liechtenstein, and Norway.

Explicit Consent: consent which requires a very clear and specific statement (not just action).

General Data Protection Regulation (GDPR): General Data Protection Regulation. Personal data is subject to the legal safeguards specified in the GDPR.

Personal Data: is any information relating to an identified or identifiable natural person (data subject) who can be identified, directly or indirectly by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (e.g., a name, email address, location, or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when the Trust collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (e.g., a Trust workforce privacy policy) or they may be stand-alone privacy statements covering processing related to a specific purpose.

Processing: means anything done with personal data, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, use, disclosure, dissemination, or otherwise making available, restriction, erasure, or destruction.

Processor: means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the data controller.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be separately and secure.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and personal data relating to criminal offences and convictions.

Subject Access Request (SAR): the right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data, as well as other supplementary information. It helps individuals to understand how and why you are using their data, and check you are doing it lawfully.