

Aletheia Anglican Academies Trust



Data Protection Policy

Review Body:	Board of Trustees
Leadership Grp Responsibility:	Chief Finance Officer
Policy Type:	Statutory
Adopted:	November 2017
Date of next review:	Spring 2018 (Due to GDPR – May 2018)
Review period:	2 years

This procedure was adopted by the Board of Trustees of Aletheia Anglican Academies Trust, for implementation in all Trust academies on the date above and supersedes any previous Data Protection Policy.

CONTENTS:

1. Introduction
2. Linked Policies
3. Responsibilities
4. Definitions
5. Data Protection Requirements
6. Notification
7. Data Gathering
8. Data Storage
9. Data Checking
10. Data Disclosure
11. Data Subject Access Requests
12. Freedom of Information Requests
13. Destroying Data
14. Breach of the Policy
15. Monitoring, Evaluation and Review

Appendices: Privacy Notices

1. Introduction

This policy is required by law. The Aletheia Anglican Academies Trust (The Trust) will publicise this policy on the Trust and individual academy websites.

The Trust processes Personal Data (as defined below) in order to enable it to provide education and other associated functions (and, additionally, where there is a legal requirement to process the personal data to ensure that it complies with its statutory obligations). This Data Protection Policy ("Policy") regulates the way in which the Trust obtains, uses, holds, transfers and processes Personal Data about individuals (including staff, learners, parents or carers and other individuals who come into contact with the Trust) and ensures all of its staff know the rules for protecting Personal Data. Further, it describes individuals' rights in relation to their Personal Data processed by the Trust.

The Trust has practices in place in relation to its handling of personal information to ensure that the Trust and its staff are acting in accordance with UK laws and regulatory guidance. These practices, together with this Policy and the Freedom of Information Policy ensure that all staff of the Trust fully understand the Trust's obligation to abide by the data privacy laws and regulations of the UK.

The Trust is committed to complying with data protection legislation at all times and all its staff are required to comply with this Policy. This policy was informed by the Information Commissioners Office official guidance for public sector organisations concerning Data Protection in Education (www.ico.gov.uk).

2. Linked Policies

This policy relates to all the Trust and academy policies which involve the collection and storage of information about people. There is also a separate

- publication schedule relating to Freedom of Information
- CCTV policy
- Whistleblowing policy
- Safeguarding and Child Protection Policy

3. Responsibilities

Under the multi academy trust arrangements, the Trust is responsible for the activities of all of the Academies within the Trust, even though some functions may have been delegated to the local Headteacher / Head of School or Local Governing Bodies. The Trust is the Data Controller for the purposes of the Act and therefore the Trustees will have overall responsibility for compliance with the DPA.

As the academies within the MAT are not separate legal entities, academies within the MAT are shown as trading names on the MAT entry.

The Trustees have delegated responsibility to the Headteacher in each academy for ensuring compliance with the DPA and this policy within the day to day activities of the academy. The Headteacher / Head of School will appoint a Data Protection Officer (DPO) for each academy.

The annual registration of academies within the Trust with the Information Commissioner's Office (ICO) is renewed by the Chief Finance Officer (CFO).

The DPO is responsible for:

- keeping the ICO up to date with changes in how the academy processes data - obtaining consent for disclosure of Personal Data, including routine consent from parents and pupils for using photographs for general academy purposes.
- ensuring data protection statements are included on forms that are used to collect Personal data.
- acting as a central point of advice for staff on data protection matters, co-ordinating requests for personal data.
- arranging appropriate data protection training for staff.
- keeping up to date with the latest data protection legislation and guidance.
- ensuring adequate systems are in place for compliance with this policy.

4. Definitions

“Personal Data Information” is any information (for example, a person's name) or combination of information about a living person which allows that living person to be identified from that information (for example a first name and an address). Examples of personal data the Trust may use include names of staff and pupils, dates of birth, addresses, national insurance numbers, academic marks, medical information, exam results, SEN assessments, staff development reviews, payroll and salary details, business interests, disciplinary and attendance records, vetting checks, and images obtained through CCTV. "Sensitive Personal Data" is Personal Data about a person's race or ethnicity, their physical or mental health, their sexual preference, their religious beliefs, their political views, trade union membership or information accusing an individual of any crime, or about any criminal prosecution against them, and the decision of the court and any punishment.

What Activities are regulated by this Policy?

The Trust processes Personal Data (including Sensitive Personal Data, see below for more information) of individuals including its staff, learners, parents or carers, contractors, business contacts, customers, suppliers and any other individuals who come into contact with the Trust, including job applicants, former staff, prospective and former learners, depending on the relationship with them, for a number of purposes, including:

- i. provision of education and other associated functions;
- ii. personnel record keeping and management;
- iii. employee performance management and professional development;
- iv. employee benefits and succession planning;
- v. payroll and pensions;
- vi. contract performance, including buying and selling goods and services;
- vii. recruitment;
- viii. business and market development;
- ix. building and managing external relationships;
- x. research and development;
- xi. work and business project scheduling;
- xii. knowledge management;
- xiii. compliance programs and policies;
- xiv. security and the prevention of crime; and
- xv. other purposes required by law or regulation and/or as notified to you separately from time to time.

When the Trust collects, stores, uses, discloses, updates or erases Personal Data for any of these purposes, this is called "Processing". If you make use of Personal Data (e.g. read, amend, copy, print, delete or send Personal Data to another organisation, whether to another academy within the Trust or otherwise) this is also a type of Processing and is subject to the guidelines set out in this Policy. We may share Personal Data with Academies within the Trust. We may also share Personal Data with any third party service providers, such as in relation to our human resources information systems, or other service providers, which we appoint in the future to Process Personal Data on behalf of the Trust.

Where collected, Sensitive Personal Data should not be used unless strictly necessary. Extra care must be taken with it (in addition to the normal rules for Personal Data) and it must be kept more securely. Additional restrictions are placed on top of the lawful reasons for Processing Personal Data mentioned above. For example, it is difficult to lawfully use such details without the consent of the individual, which has to be explicit, free, voluntary, in writing and obtained prior to Processing any Sensitive Personal Data. The Trust does not generally seek to obtain Sensitive Personal Data unless:

- i. the individual concerned agrees in writing that we may do so, on the basis of a full understanding of why the Trust is collecting the data
- ii. to monitor learners' attendance and the reasons for non-attendance
- iii. the Trust needs to do so to meet its obligations or exercise its rights under employment law and/or pastoral duties on behalf of learners
- iv. in exceptional circumstances such as where the Processing is necessary to prevent and/or detect crime or to protect the vital interests of the individual concerned (ie in "life or death" circumstances)

Staff should note that the "legitimate interest" criteria described alone is not enough to process Sensitive Personal Data.

Sensitive Personal Data should not be emailed or disclosed unless measures are taken to encrypt or otherwise secure that information due to the potential for harm or distress if the email is received by unintended recipients or otherwise goes astray. Sensitive Personal Data should be collected and used as little as possible, be kept separate from other details, be subject to more limited and strictly need to know access and used subject to greater security measures than other details

5. Data Protection Requirements

The DPA stipulates that anyone processing Personal Data must comply with eight principles of good practice. The principles require that Personal Data:-

- shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met.
- be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
- be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed.
- be accurate and where necessary, kept up to date.
- not be kept for longer than is necessary for that purpose or those purposes.
- be processed in accordance with the rights of data subjects under the Act.
- be kept secure e.g. protected by an appropriate degree of security,
- not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

6. Notification

The laws governing how we can use Personal Data apply whether the Personal Data is stored electronically (for example, in emails, on IT systems, as part of a database or in a word processed document) or in structured paper records (for example, in paper files, card indexes or filing cabinets). Data protection laws are enforced in the UK by the Information Commissioner's Office ("ICO"). The Trust maintains a notification with the ICO which sets out how it Processes Personal Data and for what purposes. The Trust shall ensure that this notification is kept up to date and renewed annually.

7. Data Gathering

Whenever the Academy collects new information about individuals we will ensure individuals are made aware:

- that the information is being collected,
- of the purpose that the information is being collected for,
- of any other purposes that it may be used for,
- with whom the information will or may be shared, - and how to contact the Data Controller.

The Trust will only obtain relevant and necessary Personal Data for lawful purposes and will only process the data in ways which are compatible with the purpose for which it was gathered. Data Privacy statements should be included on the websites and on forms that are used to collect personal data.

8. Data Storage

Personal Data will be stored in a secure and safe manner. The following measures are taken to help ensure this:

- electronic data will be protected through secure password, encryption software and firewall systems operated by the Trust.
- computer workstations in administrative areas will be positioned so that they are not visible to casual observers.
- manual Personal Data will be stored securely where it is not accessible to anyone that does not have a legitimate reason to view or process the data.
- particular attention will be paid to the need for security of Sensitive Personal Data, for example health and medical records will be kept in a locked cupboard.
- Personal Data will not be left out visible on desks.
- the physical security of academy buildings and storage systems will be regularly reviewed.
- Staff will be trained on this policy and related data protection procedures.

9. Data Checking

Systems will be put in place to ensure the Personal Data that the Trust holds is up to date and accurate. For example the Trust/Academies will ensure that parents are asked at least once a year to confirm their contact details. Any inaccuracies discovered or reported will be rectified as soon as possible.

10. Data Disclosure

We sometimes need to share the personal information we process with the individual and also with other organisations. Where this is necessary we are required to comply with all aspects of the Data Protection Act (DPA). What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons. Where necessary or required we share information with:

- family, associates and representatives of the person whose personal data we are processing
- educators and examining bodies
- careers service
- academy boards
- local and central government
- academy trusts
- healthcare, social and welfare organisations
- police forces, courts
- current, past or prospective employers
- voluntary and charitable organisations
- business associates, professional advisers
- suppliers and service providers
- financial organisations
- press and the media

Personal Data will only be disclosed to organisations or individuals for whom consent has been given to receive their data, or organisations that have a legal right to receive the data without consent being given. When requests to disclose Personal Data are received by telephone, the Academies will ensure that the caller is entitled to receive the data and that they are who they say they are. In some circumstances the Academy may call the caller back to check the identity of the caller. Personal Data will not be included on the website, in newsletters or to other media without consent of the individual (or his/her parents where appropriate). Routine consent may be requested from parents to avoid the need for frequent, similar requests for consent being made by the Academies.

11. Data Subject Access Requests

Any person whose Personal Data is held by the Trust is entitled, under the DPA, to ask for access to this information. The request must be in writing. The right is to view or be given a copy of the Personal Data, rather than to the whole document which contains Personal Data. There are some exceptions to the rights of access to information in certain records held by the Academy (e.g. in

Page 7 of 8

relation to examination scripts, legal advice). When a request is received by a member of staff, this should be passed to the Academy's Data Protection Officer without delay. The request must be dealt with promptly; a response must be provided as soon as possible and no later than within 40 calendar days from the date the request was received. The Trust may make a charge of £10 for responding to a request for Personal Data under the DPA and will need to confirm the requester's identity. A record will be kept of all data subject access requests made that require formal consideration.

12. Freedom of Information Requests

Any Freedom of Information Requests received by the Trust or Academies must be forwarded immediately to the CFO who will ensure they are dealt with appropriately.

13. Destroying Data

Out of date information will be discarded if no longer relevant. Personal Data will only be kept for as long as reasonably needed, for legal or business purposes.

14. Breach of the Policy

Non-compliance of this policy and data protection legislation by a member of staff is considered a disciplinary matter which, depending on the circumstances, could lead to dismissal.

15. Monitoring, Evaluation and Review

The DPO will monitor the implementation and effectiveness on this policy and report his/her evaluation to the CFO on an annual basis. The CFO will report back to the Trust Board on the policy and its implementation and effectiveness every two years, who will then review the policy, making any amendments necessary.