DATA PROTECTION POLICY

Approved by:	Board of Directors
Date:	July 2018
Review Date:	July 2020

Document Detail	
Document Type:	Compliance Policy
Document Name:	Data Protection Policy
Purpose:	To ensure compliance with obligations as set of in Data Protection legislation.
Version Number	1.0
Effective from:	1 September 2018
Owner:	Director of Operations
Approved by	Accord Board of Directors
Last Review	N/A
Status:	
Next Review Date:	1 September 2019
Consultation:	

Change History		
Date	**Change Details**	**Approved by**

1.0 Introduction

1.1 The Accord Multi Academy Trust is a single legal entity, therefore references to "the Trust" in this policy should be considered as inclusive of its academies.

1.2 The Trust aims to ensure that all personal data collected about staff, students, parents, trustees (directors), governors, volunteers and visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

1.3 The Trust collects and uses certain types of personal information in order to provide education and associated functions. The Trust may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding.

1.4 This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2.0 Legislation and Guidance

2.1 This policy meets the requirements of the GDPR and the expected 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.

2.2 It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

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

2.4 In addition, this policy complies with our funding agreement and articles of association

3.0 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.
Term	Definition

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.

4.0 The Data Controller

4.1 All academies within the Trust process data relating to parents, pupils / students, staff, governors, visitors and others, and as they are all part of the Accord Multi Academy Trust, it is the data controller.

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

5.0 Roles and Responsibilities

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

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

5.3 The Trust Board of Directors

5.3.1 The Board has overall responsibility for ensuring that the Trust and its academies comply with all relevant data protection obligations

5.4 Data Protection Officer

5.4.1 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.

5.4.2 They will provide an annual report of their activities directly to the Board and, where relevant, report to the Board their advice and recommendations on Academy data protection issues.

5.4.3 The DPO is also the first point of contact for individuals whose data the Trust processes, and for the ICO. Full details of the DPO's responsibilities are set out in their job description.

5.4.4 The Trust DPO is the Director of Operations and is contactable via dataprotection@accordmat.org.uk

5.5 **CEO / Principal / Headteacher**

5.5.1 The CEO (for Trust matters) and the Principal/Headteacher of each academy will act as the representative of the data controller on a day-to-day basis.

5.6 **All Staff**

5.6.1 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 DPO in the following circumstances:
  - with any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure;
  - if they have any concerns that this policy is not being followed;
  - 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;
  - if they need to rely on or capture consent/permissions;
  - if there has been a data breach;
  - if they are unsure whether or not they have a lawful basis to use personal data in a particular way;
  - if they need to draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area.

6.0 Data Protection Principles

6.1 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.

6.2 This policy sets out how the Trust aims to comply with these principles.

7.0 Collecting Personal Data

7.1 Lawfulness, fairness and transparency

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

- the data needs to be processed so that the 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; or emergency situation;
- 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 student) has freely given clear **consent.**

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

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

7.2 Limitation, minimisation and accuracy

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

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

7.2.3 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.

7.2.4 This will be done in accordance with the Trust Retentions Policy.

7.3 Sharing personal data

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

- there is an issue with a student or parent/carer that puts the safety of our staff at risk;

- We need to liaise with other agencies – we may need to seek consent as necessary before doing this;
- Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies, educational and operational software providers. When doing this, we 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 stand-alone; agreement, to ensure the fair and lawful processing of any personal data we share;
    - only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

7.3.2 We will also share personal data with law enforcement and government bodies where we 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.

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

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

8.0 Subject Access Requests and Other Rights of Individuals

8.1 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.

8.2 Subject access requests must be submitted in writing, either by letter or email to the DPO.

8.2.1 They should include:

- name of individual;
- correspondence address;
- contact number and email address;
- details of the information requested.

8.3 If staff identify a subject access request they must immediately report it to their Principal / Headteacher and forward details of the request to dataprotection@accordmat.org.uk

8.4 **Children and subject access requests**

8.4.1 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.

8.4.2 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, subject access requests from parents or carers of students who are under the age of 12 may be granted without the express permission of the pupil / student.

8.4.3 By contrast, 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 / students who are 12 and over may not be granted without the express permission of the student.

8.4.4 A student's ability to understand their rights in respect of the above will always be judged on a case-by-case basis.

8.5 **Responding to subject access requests**

8.5.1 When responding to requests, we:

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

8.5.2 We will not disclose information if it:

- might cause serious harm to the physical or mental health of the student 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.

8.5.3 If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

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

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

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

- withdraw their consent to processing at any time;
- ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances);
- prevent use of their personal data for direct marketing;
- challenge processing which has been justified on the basis of public interest;
- request a copy of agreements under which their 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).

8.7 Individuals should submit any request to exercise these rights to the DPO.

8.8 If staff receive such a request, they must immediately forward it to their Principal / Headteacher and the DPO.

9.0 Biometric Recognition Systems

9.1 In the context of the Protection of Freedoms Act 2012, a “child” means a person under the age of 18. Where we use students’ biometric data as part of an automated biometric recognition system (for example, students use fingerprints to receive school dinners instead of paying with cash, we will comply with the requirements of the Protection of Freedoms Act 2012.

9.2 Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it.

9.3 The Trust will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

9.4 Parents/carers and students have the right to choose not to use the Trust’s biometric system(s).

9.5 We will provide alternative means of accessing the relevant services for those pupils / students. For example, students can receive a pin number to pay for transactions at the till.

9.6 Parents/carers and pupils / students can object to participation in the Trust's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

9.7 As required by law, if a pupil / student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's / student's parent(s)/carer(s).

9.8 Where staff members or other adults use the Trust's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the Trust will delete any relevant data already captured.

10.0 CCTV

10.1 We use CCTV in various locations to ensure it remains safe.

10.2 We will adhere to the ICO's code of practice for the use of CCTV.

10.3 We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded.

10.4 Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

10.5 Any enquiries about academy CCTV systems should be directed to the academy themselves.

10.6 Any enquiries about CCTV at other locations should be sent to dataprotection@accordmat.org.uk

11.0 Photographs and videos

11.1 As part of our regular activities, we may take photographs and record images of individuals within the Trust.

11.2 We will obtain written consent from parents/carers, or pupils / students aged 13 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

11.3 We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil / student. Uses may include:

- within academies on notice boards and in academy magazines, brochures, newsletters, etc;
- outside of school by external agencies such as the Trust appointed photographers, newspapers, campaigns;
- on-line on the Trust websites or social media pages Consent can be refused or withdrawn at any time.

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

11.5 If consent is withdrawn, we will delete the photograph or video and not distribute it further.

12.0 Data protection by design and default

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

- appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge;
- only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6);
- completing privacy impact assessments where THE 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 the 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.

13.0 Data security and storage of records

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

- paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use;
- papers containing confidential personal data must not be left on office and classroom desks, on staff room tables, pinned to notice/display boards, or left anywhere else where there is general access;
- complex passwords must be used to access the Trust computers, laptops and other electronic devices. A password can be classed as complex when it is at least 8 characters long, contains letters and numbers and at least one special character. Staff and students will be prompted to change their passwords at regular intervals;
- encryption software is used to protect portable devices and removable media, such as laptops and USB devices as per the Trust Security Policy;

- Staff, pupils / students or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see the Trust Security Policy for more information).

13.2 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).

14.0 Disposal of records

14.1 Personal data that is no longer needed will be disposed of securely.

14.2 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 paper-based records, and overwrite or delete electronic files.

14.3 We may also use a third party to safely dispose of records on the Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

14.4 See the Trust Retentions Policy for more information on our retention periods.

15.0 Personal Data Breaches

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

15.2 In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1. When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in an educational context may include, but are not limited to:

- a non-anonymised data set being lost, or published accidentally;
- safeguarding information being made available to an unauthorised person;
- the theft of a school laptop containing non-encrypted personal data about students.

16.0 Training

16.1 All staff and governors 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.

17.0 Links with other Policies

17.1 This data protection policy is part of the Trust Information Governance Framework and is linked to our:

- Freedom of information and publication scheme

- IT Security Policy
- Retentions Policy
- Information Training Policy

18.0 Policy Review

18.1 This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018), if any changes are made to the bill that affect the Trust's practice. Otherwise, or from then on, this policy will be reviewed every 2 years and shared with all academies.

Signature: **Chief Executive**	 A Warboys
Signature: **Chair of Board of Directors**	 B Kelly
Date:	July 2018

Appendix 1: Accord Multi Academy Trust Personal Data Breach Notification Procedure

1.0 Scope

1.1 This procedure applies in the event of a personal data breach under Article 33 of the GDPR – Notification of a personal data breach to the supervisory authority – and Article 34 – Communication of a personal data breach to the data subject.

1.2 The Accord Multi Academy Trust is the legal entity for all of its academies, therefore this procedure is to be used by the organisation as a whole.

1.3 Responsibility All users (whether Employees/Staff, contractors or temporary Employees/Staff and third party users) of the Trust are required to be aware of, and to follow this procedure in the event of a personal data breach.

1.4 All Employees/Staff, contractors or temporary personnel are responsible for reporting any personal data breach to the DPO immediately after becoming aware.

2.0 Breach

2.1. With any breach, the Data Protection Officer (DPO) will investigate the report, and determine whether a breach has occurred.

2.2 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

2.3 The DPO will document each breach, irrespective of whether it is reported to the ICO.

2.4 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)

3.0 Procedure where the Trust is acting as a Data Controller

3.1 The DPO will work out whether the breach must be reported to the Information Commissioner's Office (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 non-material damage (e.g. emotional distress), including through:

- loss of control over their data
- discrimination
- identity 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

3.2 If a risk to data subject(s) is likely, the Trust will report the personal data breach to the Information Commissioner's Office (ICO) without undue delay, and not later than 72 hours.

3.3 If the data breach notification to the supervisory authority has not been made within 72 hours, the DPO will submit it electronically with a justification for the delay.

3.4 If it is not possible to provide all of the necessary information at the same time the Trust will provide the information in phases without undue further delay.

3.5 The following information needs to be provided to the supervisory authority:

- a description of the nature of the breach.
- the categories of personal data affected.
- approximate number of data subjects affected.
- approximate number of personal data records affected.
- name and contact details of the DPO.
- known consequences, likely consequences and possible future consequences of the breach.
- any measures taken to address the breach.
- any further information relating to the data breach.

3.6 The DPO will notify the ICO. In the event the ICO assigns a specific contact in relation to a breach, these details are recorded in the Internal Breach Register.

4.0 Procedure where the Trust is acting as a Data Processor

4.1 The Trust must report any personal data breach or security incident to the data controller without undue delay. These contact details must be reported to the DPO who will record the breach in the Internal Breach Register. The Trust will then provide the controller with all of the details of the breach. The breach notification is made by phone call and a confirmation of receipt of this information must be made by email.

5.0 Procedure for notification of a breach to the data subject(s)

5.1 If the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, The Trust will notify the data subjects affected immediately and without undue delay.

5.2 The notification to the data subject describes the breach in clear and plain language, in addition to information specified in clause 4 above.

5.3 The Trust will take whatever measures it can to render the personal data unusable to any person who is not authorised to access.

5.4 If the breach affects a high volume of data subjects and personal data records, the Trust will make a decision based on assessment of the amount of effort involved in notifying each data subject individually, and whether it will hinder

the Trust's ability to appropriately provide the notification within the specified time frame. In such a scenario a public communication or similar measure may be used to inform those affected in an equally effective manner.

5.5 If the Trust has not notified the data subject(s), and the ICO considers the likelihood of a data breach will result in high risk, the Trust will then seek to communicate the data breach to the data subject accordingly.