LEADING SUCCESS | SECURING SUCCESS | DEVELOPING SUCCESS | STANDARDS FOR SUCCESS | SUPPORTING SUCCESS | ACHIEVING SUCCESS

DATA PROTECTION POLICY

Accord MULTI ACADEMY TRUST

Document Detail	
Document Type:	Compliance Policy
Document Name:	Data Protection Policy
Purpose:	To ensure compliance with obligations as set out in Data Protection legislation.
Version Number:	4.0
Effective from:	01 November 2024
Owner:	Chief Operating Officer (Data Protection Officer)
Approved by:	Audit & Risk Accord Board of Trustees
Last Review:	1 November 2024
Next Review Date:	1 November 2026
Consultation:	Board of Trustees

Approvals			
Name	**Position**	**Signature**	**Date**
Alan Warboys	CEO	A Warboys	11 November 2024
Andy Lancashire	Chair of Trustees	A Lancashire	11 November 2024

Document History		
Date	**Change Details**	**Approval**
7 December 2020	Changes to wording, SARs, CCTV recordings, consent for photographs.	Board of Trustees
1 November 2022	General updates throughout in relation to legislation, procedure or additional details for clarity.	Audit & Risk Committee

1 November 2024	Additional section regarding the use of Artificial Intelligence (AI)	Audit & Risk Committee

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, pupils/students, parents, Trustees, Governors, volunteers, visitors and other individuals is collected, stored and processed in accordance with UK General Data Protection Regulations (UK GDPR) and the 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 UK GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on GDPR and the ICO's Code of Practice for Subject Access Requests and the ICO Self-Assessment Toolkit https://ico.org.uk/for-organisations/sme-web-hub/checklists/data-protection-self-assessment/.

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.
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, Trustees, 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 Board of Trustees

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 / Trust 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 Chief Operating Officer and is contactable via dataprotection@accordmat.org.

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, processing and safe disposal of 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 have received a data subject access request (DSAR);
- 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;
- accountable for by the data controller to ensure compliance with and demonstration of compliance with the above principles.

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 pupil/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 under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

7.1.3 For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation.

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

7.1.5 We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

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 – a copy of which can be found on SharePoint or by request from dataprotection@accordmat.org.

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 pupil/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 pupils/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, for example but not limited to for the following reasons:

- 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 pupils/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. Where there are changes to legislation or the European Economic Area this policy will be updated accordingly.

7.3.5 Full details of how we will collect and share personal data can be found in our Privacy Notices which can be found on the Trust website at https://accordmat.org/keyinformation/.

7.3.6 Colleagues who are permitted to share personal data in line with this policy with for example other internal colleagues, with external third parties or parents/carers must do so using the Trust approved secure processes i.e. a SharePoint or OneDrive link to a file or document which is restricted to specific people or email addresses, a password protected file or attachment.

8.0 Data Subject Access Requests (DSAR) and Other Rights of Individuals

8.1 Individuals have a right to make a 'Data 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 will generally be submitted in writing, either by letter or email to the DPO. However verbal requests for data may also be received. If this occurs colleagues should follow up with the individual making the request, to ask that they submit their access request in writing.

8.2.1 Subject access requests should include:

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

8.2.2 For academies, including free schools, and independent schools - there is no automatic parental right of access to the educational record, but we may choose to provide this.

8.3 If staff identify a subject access request they must immediately report it to their Principal / Headteacher, the academy PA to Principal / Office Manager and forward details of the request to the DPO at dataprotection@accordmat.org.

8.4 Where the request is in relation to safeguarding the academy DSL must also be made aware.

8.5 The academy PA to Principal / Office Manager will coordinate responding to the request, gathering the requested information and ensuring the information is redacted where necessary prior to sending the response. Support will be provided by the DPO.

8.6 Colleagues dealing with a subject access request can refer to the procedure documentation for clarity and frequently asked questions available from the DPO at dataprotection@accordmat.org.

8.7 **Children and Subject Access Requests**

8.7.1 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.

8.7.2 Children aged 12 and below 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/students or carers of pupils who are age 12 and below may be granted without the express permission of the pupil / student.

8.7.3 By contrast, children aged 13 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 / pupils who are 13 and over may not be granted without the express permission of the pupil/student. A pupil will be asked to sign a specific permission form in the presence of two impartial members of staff i.e. DPO, Principal or a representative.

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

8.8 **Responding to Data Subject Access Requests (DSAR's)**

8.8.1 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;
- if the deadline day falls on a weekend the deadline will be the next working day;
- 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. (Where this may apply we will inform the individual of this within 1 month, and explain why the extension is necessary.)
- **Note** – working days are all days Monday to Friday, the timeframe for response does not pause for academy holiday periods.

8.8.2 We will not disclose information if it:

- might cause serious harm to the physical or mental health of the pupil or another individual;
- would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests;
- is contained in adoption or parental order records;
- is given to a court in proceedings concerning the child.

8.8.3 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.

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

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

8.8.6 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).

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

8.8.8 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 pupils’ biometric data as part of an automated biometric recognition system (for example, pupils 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 obtain written consent from at least one parent, carer or person with parental responsibility before we take any biometric data from their child and first process it.

9.4 Parents/carers and pupils/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 / pupils. For example, pupils can receive a pin number to pay for transactions.

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 the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's/ pupil'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.

9.9 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 Trust sites remain safe.

10.2 CCTV is recorded and stored for seven days and is only accessed for viewing for investigative purposes. As CCTV has the potential to cover a number of data subjects, it is not routinely disclosed.

10.3 We will adhere to the Government's code of practise for the use of CCTV which can be found at https://www.gov.uk/government/publications/update-to-surveillance-camera-code/amended-surveillance-camera-code-of-practice-accessible-version.

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

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

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 / pupils aged 13 and over, for photographs and videos to be taken of pupils 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.

11.4 At the time of the photograph / video being taken we will seek verbal consent from pupils/students to allow them to withdraw consent at that time.

11.5 Uses of photos/videos 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 by contacting the academy.

11.6 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 other than for example the use of initials or strictly first name only.

11.7 When consent is withdrawn, or if we receive a request for the right to be forgotten, the Trust will delete the photograph or video and not distribute further, however in pre-published documentation this will be withdrawn at the next publication point (e.g. prospectus).

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 DPIA (Data 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 with the support of the Director of ICT);
- 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 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 when using a Trust issued user account and any other software or system associated with the Trust. The password policy is set out in detail in the Acceptable Use Policy;
- encryption software is used to protect portable devices and removable media, such as laptops as per the Trust Acceptable Use Policy;
- USB devices are no longer permitted at the Trust;
- staff, pupils, Governors or Trustees who access personal information via Trust systems on their personal devices are expected to follow the same security;

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 shared securely and adequately protected.

14.0 Artificial Intelligence (AI)

Under no circumstances should personal or identifying information about staff, pupils or other individuals be entered into any AI system without prior agreement from the Data Protection Officer (DPO). In these circumstances, a Data Protection Impact Assessment (DPIA) will be carried out to ensure that appropriate levels of data and cyber security are present to protect personal information.

Any AI systems created by the Trust should be stored within the Trust's closed infrastructure, stored in data centres compliant under GDPR.

15.0 Disposal of Records

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

15.2 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.

15.3 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.

15.4 The Trust Retentions Policy details the principles that the Trust follow for retention and destruction of information and data and our retention periods.

15.5 Staff are required to undertake a data audit on a regular basis to ensure data is only retained in line with the Trust Retention Policy.

16.0 Personal Data Breaches

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

16.2 In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1. When appropriate, the DPO will report the data breach to the ICO within 72 hours.

16.3 The Trust DPO maintains a Data Breach Log of all breaches, whether reportable or not to the ICO.

17.0 Training

17.1 All staff, Trustees and Governors are provided with data protection training relevant to their role as part of their induction process.

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

18.0 Links with other Policies

18.1 This Data Protection Policy is a statutory policy and should be read in conjunction with:

- Freedom of Information Policy;
- Retentions Policy;
- Privacy Notices;
- Staff Code of Conduct;
- Acceptable Use Policy;
- Artificial Intelligence Usage (AI) Policy.

19.0 Policy Review

19.1 This policy will be reviewed every 2 years or as changes to legislation or procedure require it.

20.0 Contact Information

Name	**Email / Website:**	**Tel:**
Chief Operating Officer / Data Protection Officer (DPO)	dataprotection@accordmat.org	01924 668936

Appendix 1:

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 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 All users (whether employees / staff, Governors, Trustees, 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, Governors, Trustees, contractors or temporary personnel are responsible for reporting any personal data breach to the Data Protection Officer (DPO) immediately after becoming aware.

2.0 Breach

2.1. With any suspected breach, the 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 Information Commissioner's Officer (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).

2.5 All reported incidents or near misses will be logged for training purposes and will be shared periodically through Academy Education Committee Reports and to the Board of Trustees.

3.0 Procedure where the Trust is acting as a Data Controller

3.1 The DPO will determine through undertaking a risk assessment whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To determine, 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 ICO without undue delay, and no later than 72 hours.

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

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 in line with the ICO procedure.

3.5 The following information needs to be provided to the ICO when a breach is reportable:

- 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 In the event the ICO assigns a specific contact in relation to a notification of a breach, these details will be recorded on the Trust Data 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 on the Trust Data 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 there is a high risk of detriment to the data subject's rights and freedoms following a personal data breach, 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 how it has occurred and what the Trust has done to rectify and/or ensure a similar type of breach does not occur again.

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 as advised by the ICO.