Data Protection Policy

Designation	Name	Date	Signature
CEO:	Mrs Lyn Dance		
Chair of Trust Board:	Mr David Ellis		

SAND Academies Trust
Lyn Dance CEO & Executive Headteacher
Registered in England: Company Number 11968610
Registered Office: The Milestone School, Longford Lane, Gloucester, GL2 9EU - Telephone: 01452 874000 – www.sandmat.uk

Monitoring and Evaluation	
Original implementation date:	April 2021
Review frequency:	Annually
Date of next Review:	April 2022
Review delegated to:	

Document Version control

Version	Changes made	Date
1.0	Initial set up of Trust-wide policy	April 2021

SAND Academies Trust
Lyn Dance CEO & Executive Headteacher
Registered in England: Company Number 11968610
Registered Office: The Milestone School, Longford Lane, Gloucester, GL2 9EU - Telephone: 01452 874000 – www.sandmat.uk

1. Aims

SAND Academies Trust aims to ensure that all personal data collected about staff, pupils, parents, board members, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA). This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Background

The law changed on 25 May 2018 with the implementation of GDPR – an EU law that is directly effective in the UK, regardless of Brexit status – and a new Data Protection Act that was also passed to deal with certain issues left for national law. In most ways this law has strengthened the rights of individuals and placed tougher compliance obligations on organisations, including schools that handle personal data. This policy meets the requirements of GDPR and the DPA.

The Information Commissioner's Office (ICO) is responsible for enforcing data protection law. Typically, it will routinely look into individuals' complaints without cost and has various powers to act for breaches of data protection law. The ICO also publishes guidance and codes of practice for organisations, which are available on its website. This policy was written with regard to this information. In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005 which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data (or personal information)	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include job titles and nicknames and 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 • Sex life or sexual orientation • Health or medical conditions – physical or mental There are also separate rules for the processing of personal data relating to criminal convictions and offences.
Processing	Virtually anything done to personal data, such as collecting, recording, organising, sharing, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying it. 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, and is legally responsible for how it is used.
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, for example a payroll or IT provider.
Personal data breach	A breach of security leading to the Accidental or unlawful destruction, loss, alteration,unauthorised disclosure of, or access to personal data.

4. The data controller

Our *school* processes personal data relating to parents, pupils, staff, board members, visitors and others, and therefore *are* data controllers and is registered as data controller with the Information Commissioner's Office (ICO). We will renew this registration annually or as otherwise legally required.

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

5. Roles and responsibilities

This policy sets out the school's expectations and procedures with respect to processing any personal data we collect from data subjects (including parents, pupils, employees, contractors and third parties).

This policy applies to all staff employed by our school. Staff who do not comply with this policy may face disciplinary action. Accidental breaches of the law or this policy in handling personal data will happen from time to time(by human error, for example) and will not always be treated as a disciplinary issue. However, failure to report breaches that pose significant risks to the school or individuals will be considered a serious matter.

In addition, this policy represents the standard of compliance expected of those who handle the school's personal data as contractors, whether they are acting as "data processors" on the school's behalf (in which case they will be subject to binding contractual terms) or as data controllers responsible for handling such personal data in their own right.

5.1 Trust Board

The Trust Board has overall responsibility for ensuring that all our school complies with all relevant data protection obligations.

5.2 Data protection officer

Our 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. The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Our area DPO Antonia Noble (Carter Noble Independent Safeguarding) is contactable via email (antonia@carter-noble.co.uk or antonia.noble@icloud.com) or phone (07824665908).

The school is committed to ensuring its staff are aware of data protection policies, legal requirements and are adequately trained; we do this together with our Data Protection Officer. The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

5.3 All staff are responsible for:

- Collecting, storing, using, processing and sharing (where appropriate and agreed) any personal data in accordance with this policy
- Informing the school 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
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals or
    - If they need help with any contracts or sharing personal data with third parties.

6. Data protection principles

GDPR is based on data protection principles that our school must comply with. These require that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure.

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

GDPR's broader 'accountability' principle also requires the school to not only process personal data in a fair and legal manner but also to *demonstrate* that our processing is lawful. This involves, among other things:

- Keeping records of our data processing activities, including logs and policies
- Documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments)
- Generally having an 'audit trail' vis-à-vis data protection and privacy matters, including, for example, when and how our Privacy Notice(s) were updated; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.

7.Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of six legal bases to do so under data protection law:

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract, e.g. in connection with employment and engagement of services
- The data needs to be processed so that the school can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, 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 school or a third party (but only if the impact on the individual's privacy rights and freedoms are justified)
- The individual (or their parent/carer/those with parental responsibility when appropriate in the case of a pupil) has freely given clear consent.

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 DPA.

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

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 if we have not done so before – this is normally done through our data privacy notices. 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 where necessary. Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised in line with this policy.

8. Sharing personal data

We will share personal data where:

- There is an issue with a pupil or parent/carer/those with parental responsibility that puts the safety of anyone at risk
- We need to liaise with other agencies (please see below for further information)
- Our suppliers or contractors require data to enable us to provide services to our staff and/or pupils; any volunteers including governors or parents/cares or those with parental responsibility – for example, IT and cloud service provider companies. When doing this, we will:

(a) Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
(b) Establish a data processing contract or agreement with the supplier or contractor, either in the contract or as a standalone agreement
(c) 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.

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
- We may also share personal data with emergency services and local authorities. For instance, to help them to respond to an emergency situation that affects any of our pupils or staff.

Personal data may be shared with the following third parties without consent:

Other schools

If a pupil transfers to another school, their academic records and other data that relates to their health and welfare (including any Child Protection and Safeguarding files) will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

Examination authorities

This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

Health authorities

As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

Police and courts

If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

Disclosure and Barring Service

Where appropriate we may share data with the DBS for example if there is a relevant safeguarding concern about an adult connected to the school.

Social workers and support agencies

In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

Department for Education and local authority

The school may be required to pass data on in order to help the government monitor the national educational system and enforce laws relating to education.

9. Data Subject Access Requests (Subject Access Requests) and other rights of individuals

9.1 Data Subject Access Requests

Individuals have a right to make a Data Subject Access Request to gain access to personal data or information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of their personal 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
- The safeguards we provide if the school transfers their personal data to a country outside the European Economic Area.

Data Subject Access Requests do not need any formality to be made but we ask that they include the:

- Name of the individual
- Contact information, e.g. postal or email address
- Details of the information requested.

We shall respond to such requests within one calendar month (unless it is necessary and we are permitted to extend this period) and we ask that they are made in writing to the lead for data protection within the school or our Data Protection Officer.

9.2 Data Subject Access Requests made on behalf of others

GDPR does not prevent an individual (e.g. pupil, parent or member of staff) making a request via a third party such as a family member or solicitor acting on behalf of a client. In these cases the school must be satisfied that the third party making the request is entitled to act on behalf of the individual and the third party should provide evidence of this entitlement, e.g. a written authority. Before responding to a request for information held about a pupil, the school will consider whether the pupil is mature enough and has the capacity to understand their rights. If the school is confident that the pupil can understand their rights, then we will usually respond directly to the pupil. The school may, however, allow the parent to exercise the pupil's rights on their behalf if the pupil authorises this, or if it is evident that this is in the best interests of the pupil.

9.3 Responding to Data Subject Access Requests

When responding to requests, we:

- May ask the individual to provide evidence of identity (only if necessary)
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month, and explain why the extension is necessary.

We will not disclose information where we are required or permitted to withhold it, including if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child
- Is a reference, whether academic or professional, given or received confidentially
- Is legally privileged (e.g. confidential legal advice between school and solicitor)
- Relates to management planning or forecasting (e.g. planned redundancies, management consultancy)
- Is part of confidential negotiations with the requester (i.e. the school's intentions in offering settlement).

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

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

9.4 Other data protection rights of the individual

In addition to the right to make a data subject access request (subject access request), 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 where we are relying on it for processing their personal data
- 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 or legitimate interests
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Object to processing that the individual feels has a disproportionate impact on them, e.g. is likely to cause significant damage or distress
- Be notified of a data breach in certain circumstances.

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO. Individuals not satisfied with a school's response have a right to make a complaint to the data protection regulator, the ICO.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

11. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to [name/job title].

12. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other

pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where the school takes photographs and videos, uses may include:

- Within school on displays and newsletters
- When necessary for teaching purposes –in sports or drama, for example
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website and social media - Class Dojo
- Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further

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.

Photographs or images taken of other individuals who are not pupils will always have prior consent – except those which are used as part of staff contracts and set out in our staff privacy notice.

Our child protection and safeguarding policy has more information on our use of photographs and videos.

13. Data protection by design and default

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 school'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 our school 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.

14. Data security and storage of records

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 staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

15. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it e.g. we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. Personal data breaches

Data controllers – our school – must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

In addition, data controllers must notify individuals affected if the breach is likely to result in a 'high risk' to their rights and freedoms. In any event, each school will keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If staff become aware of a personal data breach they must notify the DPO. If staff are in any doubt as to whether to report something internally, it is always best to do so. A personal data breach may be serious, or it may be minor; and it may involve fault or not; but the school always needs to know about them to make a decision.

The school may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the school, and for those affected, and could be a serious disciplinary matter whether under this policy or the applicable staff member's contract.

We maintain a data breach record; review our processes in the event of any breach and take necessary remedial action.

17. Training

All staff and board members 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 school's processes make it necessary.

18. Monitoring arrangements

The DPO is responsible for monitoring this policy. The DPO will also review this policy annually and it will be submitted to the trust board for approval.