SAND

ACADEMIES TRUST

Supporting Achievement Nurturing Development

SAND Academies Trust

Data Protection Policy

Status Statutory **X** Recommended☐ Good Practice ☐
Purpose The management of the SAND Academy Trust is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles, General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA). This Policy and Guidance takes into consideration 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. This policy complies with the regulation 5 of Education (Pupil Information) (England) Regulations 2005
Consultation Staff, board members and parents as appropriate
Links with other policies Safeguarding Policy Disciplinary Policy
Monitoring and Evaluation Annually **X** Every 3 years ☐Other☐ Headteacher ☐ Chair of SAND Academy Trust Board☐ Committee Chair ☐ Other ☐
Dates Original Implementation January 2020 Review January 2021

Contents

1. Aims

Our schools aim 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 expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

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. 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	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. The data controller

Our *schools* processes personal data relating to parents, pupils, staff, board members, visitors and others, and therefore *are* data controllers. All the schools under the SAND Academy Trust are registered as data controllers respectively with the Information Commissioner's Office (ICO) and 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.

Breaches of personal or sensitive data shall be notified within 72 hours to the individual(s) concerned and the ICO.

5. Roles and responsibilities

This policy applies to all staff employed by our schools under the Academy, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Trust Board

The Trust Board has overall responsibility for ensuring that all our schools comply with all relevant data protection obligations. This is reinforced by the Local Advisory Board of each school.

5.2 Data protection officer

The named 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. Each school has a named DPO.

Our area DPO is Gloucestershire County Council and is contactable via 01452 583619 or schoolsdpo@gloucestershire.gov.uk.

The Trust is committed to ensuring that its staff are aware of data protection policies, legal requirements and adequate training is provided by Gloucestershire County Council. The requirements of this policy are mandatory for all staff employed by the academy and any third party contracted to provide services within the schools.

5.3 Headteacher

The respective headteachers act as the representative of the data controller on a day-to-day basis who can delegate this duty to a member of their Senior Leadership Team.

5.4 All staff are responsible for:

- Collecting, storing and processing 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 o If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that our schools 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

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

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
- ❖ 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 (provided the individual's rights and freedoms are not overridden)
- ❖ The individual (or their parent/carer 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 Data Protection Act 2018.

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, minimization 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 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 anonymized.

8. Sharing personal data

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

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. 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 standalone 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

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
- 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 or staff.

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

9.1 Data Access Requests

Individuals have a right to make a data 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 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.

Data access requests should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

We shall respond to such requests within one month and they should be made in writing to:

The head teacher of the relevant SAND AT school.

9.2 Children and data access request (subject access requests)

Personal data about pupils will not be shared with third parties without the consent of the child's parent or carers, unless it is obliged by law or in the best interest of the child.

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 will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that 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 schools 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.

- ***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.

- ***Educational division***

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

- ***Right to be Forgotten***

  Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal

data is erased by the school including any data held by contracted processors.

9.3 Responding to data (subject) access requests

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

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

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 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
- 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 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.

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. Photographs and videos

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

Uses may include:

- Within school on notice boards and in school newsletters, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages
- 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.

See our child protection and safeguarding policy for more information on our use of photographs and videos.

12. 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:

    o 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)

    o 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. 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)

14. 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.

15. Personal or sensitive data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach we will report the data breach to the individual(s) concerned and the ICO within 72 hours and use appropriate disciplinary procedures in line with school policy.

16. 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.

17. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy. 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 our school's practice. Otherwise, or from then on, this policy will be reviewed every 2 years and shared with the full governing board. While the GDPR and Data Protection Act 2018 (when in place) are still new, the

school will review our data protection policy annually, and then extend this to every 2 years once we are confident with our arrangements.

Appendix A

Retention Schedule

Record Series	Trigger Point	Minimum Retention period at School	Basis for keeping records	Action
Accident Reports (children)	Date of birth of child	25 years	Limitation Act 1980, Section 2	Destroy
Accident/injury at work records (staff)	Date of incident	4 years	Limitation Act 1980, Section 11	Review
Accounting records	End of financial year	6 years	HMRC - Compliance Handbook Manual CH15400	Review: Archive annual accounts
Administrative files (routine)	End of administrative use	6 years	Limitation Act 1980, Section 2	Review
Admission registers	Date of last entry	6 years	Limitation Act 1980, Section 2	Archive
Attendance registers	End of academic year	3 years		Destroy
Contracts under seal	End of contract	12 years	Limitation Act 1980, Section 8	Destroy
Contracts under hand	End of contract	6 years	Limitation Act 1980, Section 2	Destroy
Contract monitoring records	End of Current year	2 years		Destroy
Development plans (School)	End of administrative use	6 years	Limitation Act 1980, Section 2	Archive

Examination certificates (public)				Any certificates left unclaimed should be returned to the appropriate Examination Board
Examination results - internal	End of academic year	5 years		Destroy
Examination results - public	End of academic year	6 years	Limitation Act 1980, Section 2	Destroy
Free School Meal Registers	End of current year	6 years	Limitation Act 1980, Section 2	Destroy
Governors' reports	Date of meeting	6 years	Limitation Act 1980, Section 2	Archive
Instruments of Government	Date Instruments drawn up	Retain permanently until closure of school		Archive
Log book	Date of last entry	6 years		Archive
Maintenance logs	Date of last entry	10 years	Limitation Act 1980, Section 2	Destroy
Minutes of governors, staff and PTA meetings	End of academic year	6 years	Limitation Act 1980, Section 2	Archive
OFSTED reports and papers	Superseded by new report	Review on replacement by new inspection report		Archive
Policies	Superseded by new policy			
Property title deeds and architect's plans	No longer used regularly	Permanent		Archive

Pupil files and record cards (primary)	Pupil leaves school	Immediate	Transfer records to secondary (or other primary) school	
Pupil files and record cards (secondary)	Date of birth of pupil	25 years	Limitation Act 1980, Section 2	Destroy
SATs/PAN/Value added records	End of academic year	6 years		Destroy
School Prospectus	End of academic year	3 years		
Special Educational Needs (SEN) files	Date of birth of pupil	31 years	Children and Families Act 2014; Limitation Act 1980, Section 2	Review. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case
Special Educational Needs and Disability Act 2001 Section 1: statements	Date of birth of pupil	31 years	Children and Families Act 2014; Limitation Act 1980, Section 2	Review
Staff - personnel files	End of employment	6 years	Limitation Act 1980, Section 2	Destroy