# Data Protection Policy

To be reviewed biennially or as required by changes in legislation

| | |
|---|---|
| Ref: | **005-2018 Issue 2** |
| Author: | **T Darby** |
| Issued: | **April 2018** |
| Reviewed by: | **Provision Committee** |
| Changes | **Re-write in advance of GDPR May 2018** |
| Approved by: | |
| Next review: | **Spring 2020** |
| Directors: | To be presented to Full Board for information |

**Contents**

1. Aims ..... 3
2. Legislation and guidance ..... 3
3. Definitions ..... 3
4. The data controller ..... 4
5. Roles and responsibilities ..... 4
6. Data protection principles ..... 5
7. Collecting personal data ..... 6
8. Sharing personal data ..... 6
9. Subject access requests and other rights of individuals ..... 7
10. Parental requests to see the educational record ..... 9
11. Biometric recognition systems ..... 9
12. CCTV ..... 10
13. Photographs and videos ..... 10
14. Data protection by design and default ..... 10
15. Data security and storage of records ..... 11
16. Disposal of records ..... 11
17. Personal data breaches ..... 11
18. Training ..... 12
19. Monitoring arrangements ..... 12
20. Links with other policies ..... 12
Appendix 1: Personal data breach procedure ..... 13
Appendix 2: Subject access request form ..... 16

## 1. Aims

SENDAT aims to ensure that all personal data collected about staff, pupils, parents, governors, 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.

Finally, this policy complies with our funding agreement and articles of association.

## 3. Definitions

| Term | Definition |
|---|---|
| **Personal data** | Any information relating to an identified, or identifiable, individual.<br><br>This may include the individual's:<br>• Name (including initials)<br>• Identification number<br>• Location data<br>• Online identifier, such as a username<br><br>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:<br>• Racial or ethnic origin<br>• Political opinions<br>• Religious or philosophical beliefs<br>• Trade union membership<br>• Genetics<br>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes |

| | |
|---|---|
| | • Health – physical or mental<br>• 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.<br><br>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

SENDAT ("the Trust") processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

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

### 5. Roles and responsibilities

This policy applies to **all staff** employed by SENDAT (including all its constituent Trusts and other provisions), and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

#### 5.1 Board of directors

The SENDAT Board of Directors has overall responsibility for ensuring that the Trust complies with all relevant data protection obligations.

#### 5.2 Data Protection Officer

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.

The DPO will provide an annual report of their activities directly to the board of directors and, where relevant, report to the board their advice and recommendations on Trust data protection issues.

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

Our Data Protection Officer is Sian Durrant (Trusts' Choice) and is contactable via:

- Landline: 01473 260741
- Mobile: 07720208841
- Email: sian.durrant@Trustschoice.org

**Contact with the DPO should be made via the Trust's Central Administration team in the first instance.**

Email: tracy.darby@sendat.academy
Tel: 01284 761394

**5.3 CEO**
The CEO acts as the representative of the data controller on a day-to-day basis.

**5.4 All staff**
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 Data Protection Officer 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, 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
    - 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 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

This policy sets out how the Trust 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 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
- 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) 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.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law – this will be in the form of a privacy notice.

The current privacy notices for each relevant category of data subject can be found on our website and at Appendices 3, 4 and 5 of this policy.

### 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 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. This will be done in accordance with the Information and Records Management Society's toolkit for Trusts.

## 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.

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.

## 9. Subject access requests and other rights of individuals

### 9.1 Subject access requests

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

Subject access requests must be submitted in writing to the Data Protection Officer. A template form for this purpose can be found in Appendix 2.

If staff receive a subject access request they must immediately forward it to the Data Protection Officer.

**9.2 Children and subject access requests**
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.

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. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

**9.3 Responding to 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 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)

Individuals should submit any request to exercise these rights to the Data Protection Officer.

If staff receive such a request, they must immediately forward it to the Data Protection Officer.

**10. Parental requests to see the educational record**

Parents have the right of access to their child's educational record, free of charge, within one month of receipt of the request.

**11. Biometric recognition systems**

The Trust does not currently use any biometric recognition systems. If and when such a system is put in place:

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

- Parents/carers and pupils will have the right to choose not to use the Trust's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for Trust dinners in cash at each transaction if they wish.

- Parents/carers and pupils 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.

- As required by law, if a pupil 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 parent(s)/carer(s).

- 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.

**12. CCTV**

The Trust does not currently use CCTV in any of its locations. In the event that a CCTV system were to be installed, 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 will be clearly visible and accompanied by prominent signs explaining that CCTV is in use.

**13. Photographs and videos**

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

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within Trust on notice boards and in Trust magazines, brochures, newsletters, etc.
- Outside of Trust by external agencies such as the Trust photographer, newspapers, campaigns
- Online on our Trust 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.

**14. 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:

- 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
- 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 Data Protection Officer 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 training

- 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 Trust and Data Protection Officer 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

**15. 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, unrestricted access;
- Passwords that are at least 8 characters long containing letters and numbers are used to access Trust 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 Trust-owned equipment (see our policy on acceptable use);
- 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.

**16. 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.

For example, we will shred paper-based records, and overwrite or delete electronic files. 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.

**17. Personal data breaches**

The Trust 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 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 a Trust context may include, but are not limited to:

- A non-anonymised dataset being published on the Trust website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a Trust laptop containing non-encrypted personal data about pupils

**18. Training**

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.

**19. Monitoring arrangements**

The Data Protection Officer 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 Trust's practice.

Otherwise, or from then on, this policy will be reviewed biennially or as required by changes in legislation

**20. Links with other policies**

This data protection policy is linked to our:

- SENDAT Staff Code of Conduct
- Data Retention Schedule

**Appendix 1: Personal data breach procedure**

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Data Protection Officer
- The Data Protection Officer will investigate the report, and determine whether a breach has occurred. To decide, the Data Protection Officer 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
- The Data Protection Officer will alert the CEO and the board of directors
- The Data Protection Officer will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The Data Protection Officer will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The Data Protection Officer will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the Data Protection Officer 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
    - Identify 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

  If it's likely that there will be a risk to people's rights and freedoms, the Data Protection Officer must notify the ICO.
- The Data Protection Officer will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in the Trust's data breach log.
- Where the ICO must be notified, the Data Protection Officer will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the Data Protection Officer will set out:

    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the Data Protection Officer
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the Data Protection Officer will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the Data Protection Officer expects to have further information. The Data Protection Officer will submit the remaining information as soon as possible
- The Data Protection Officer will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the Data Protection Officer will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the Data Protection Officer
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The Data Protection Officer will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The Data Protection Officer will document each breach, irrespective of whether it is reported to the ICO. 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)

  Records of all breaches will be stored on the Trust's data breach log.
- The Data Protection Officer and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

**Actions to minimise the impact of data breaches**
We will take a range of appropriate actions to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information.

We will review the effectiveness of these actions and amend them as necessary after any data breach.

**For example, sensitive information being disclosed via email (including safeguarding records)**

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the Data Protection Officer as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the Data Protection Officer will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the Data Protection Officer will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The Data Protection Officer will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The Data Protection Officer will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

**Appendix 2: Subject access request form**

| |
|---|
| **Name:** |
| **Telephone Number:** |
| **Email:** |
| **Address:** |
| **Employee Payroll Number** *(If relevant)***:** |
| By completing this form, you are making a request under the General Data Protection Regulation (GDPR) for information held about you by the Trust that you are eligible to receive. |
| **Required information (and any relevant dates):**<br><br>*Example: Emails between "A" and "B" from 1 May 2017 to 6 September 2017.* |
| By signing below, you indicate that you are the individual named above. The Trust cannot accept requests regarding your personal data from anyone else, including family members. We may need to contact you for further identifying information before responding to your request. You warrant that you are the individual named and will fully indemnify us for all losses, cost and expenses if you are not.<br><br>Please return this form via email to the Data Protection Officer on sian.durrant@Trustschoice.org<br><br>Please allow 1 calendar month for a reply. |
| **Data Subject's Signature:** |
| **Date:** |

**APPENDIX 3**
**SENDAT PUPIL PRIVACY NOTICE**

The Trust (will includes all its constituent Trusts and other specialisms) collects and processes personal data relating to its pupils in order to successfully carry out its functions. The Trust is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

**Who We Are**

Under Data Protection legislation, the Trust is a data controller.
The contact details for the Trust are as follows:
SENDAT, Mount Road, Bury St Edmunds IP32 7BH

**Our Data Protection Officer**

The Trust's Data Protection Officer is currently:
Sian Durrant (Trusts' Choice) – initial contact via the SENDAT Central Administration office.

**Categories of Information**

The Trust collects and processes a range of information about its pupils. This includes:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free Trust meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Insert additional categories of pupil information that you collect/hold and/or share. These might include; assessment information, relevant medical information, special educational needs information, exclusions/behavioural information, post 16 learning information.

**Why We Collect and Use This Information**

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing
- to safeguard and promote the welfare of pupils
- to fulfil our contractual and other legal obligations
- to provide additional activities for pupils, for example, activity clubs and educational visits
- to protect and promote our interests and objectives - this includes fundraising

- Add to this list any other reasons for which you collect and use pupil information.

**The Lawful Basis On Which We Use This Information**

We collect and use pupil information under section 537A of the Education Act 1996, and section 83 of the Children Act 1989. We also comply with Article 6(1)(c) and Article 9(2)(b) of the General Data Protection Regulation (GDPR).

**Collecting Pupil Information**

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

We may acquire Personal Data in a number of ways including, without limitation, the following:

- parents of pupils may provide us with Personal Data about themselves or their family in correspondence, forms, documents, during discussions with staff, and through our website;
- we may acquire Personal Data from other parents, or from people outside of the community who know parents or from the pupils themselves; and
- we may acquire Personal Data from third parties such as Trusts and nurseries, public authorities, public sources or from commercial sources such as credit reference agencies.

**Storing Pupil Data**

We hold pupil data for insert the length of time for which the personal data will be stored and/or include link to the Trust retention policy.

**Who We Share Pupil Information With**

We routinely share pupil information with:

- Trusts that the pupils attend after leaving us
- our local authority
- the Department for Education (DfE)
- Amend and/or extend this list to include all other parties with whom you regularly share pupil information. For example, Trust nurse or NHS etc.

**Why We Share Pupil Information**

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins Trust funding and educational attainment policy and monitoring.

We are required to share information about our pupils with the (DfE) under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

We are required to pass information about our pupils in Pupil Referral Units (PRUs) to the Department for Education (DfE) under regulation 4 of The Education (Information About Individual Pupils) (England) Regulations 2013.

**Data Collection Requirements**
To find out more about the data collection requirements placed on us by the Department for Education (for example; via the Trust census) go to https://www.gov.uk/education/data-collection-and-censuses-for-Trusts.

**Youth Support Services**

Once our pupils reach the age of 13, we also pass pupil information to our local authority and/or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers

A parent or guardian can request that only their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child/pupil once he/she reaches the age 16.

We will also share certain information about pupils aged 16+ with our local authority and/or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, please visit our local authority website.

**The National Pupil Database (NPD)**

The NPD is owned and managed by the Department for Education and contains information about pupils in Trusts in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including Trusts, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the Trust census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The DfE may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The DfE has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the DfE's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:
https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

**Requesting Access to Your Personal Data**

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, please contact insert name and contact details.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress

- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

**Further information**

If you would like to discuss anything in this privacy notice, please contact:

Mrs T Darby, Chief Finance and Operations Officer, SENDAT
Email: tracy.darby@sendat.academy
Tel: 01284 761394

**APPENDIX 4**
**SENDAT STAFF PRVACY NOTICE**

The Trust (which includes all its constituent Trusts and Specialisms) collects and processes personal data relating to its employees to manage the employment relationship. The Trust is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

**Who We Are**

Under Data Protection legislation, the Trust is a data controller.

The contact details for the Trust are as follows:
SENDAT, Mount Road, Bury St Edmunds IP32 7BH

**Our Data Protection Officer**

The Trust's data protection officer is currently:
Sian Durrant (Trusts' Choice) – initial contact via the SENDAT Central Administration office.

**Categories of Information**

The Trust collects and processes a range of information about its employees. This includes:

- your name, address and contact details, including email address and telephone number, date of birth and gender;
- the terms and conditions of your employment;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the organisation;
- information about your remuneration, including entitlement to benefits such as pensions;
- details of your bank account and national insurance number;
- information about your marital status, next of kin, dependants and emergency contacts;
- information about your nationality and entitlement to work in the UK;
- information about your criminal record;
- details of your schedule (days of work and working hours) and attendance at work;
- details of periods of leave taken by you, including holiday, sickness absence and family leave, and the reasons for the leave;
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- assessments of your performance, including appraisals, performance reviews and ratings, performance improvement plans and related correspondence;
- information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments; and
- equal opportunities monitoring information including information about your ethnic origin, sexual orientation and religion or belief.

The Trust may collect this information in a variety of ways. For example, data might be collected through application forms or CVs; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment (such as benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.

In some cases, the Trust may collect personal data about you from third parties, such as references supplied by former employers, information from employment background check providers and information from criminal records checks permitted by law.

Data will be stored in a range of different places, including in your personnel file, in the Trust's HR management systems and in other IT systems (including the Trust's email system).

**Why We Collect and Use This Information**

The Trust needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefit, pension and insurance entitlements.

In some cases, the Trust needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled.

In other cases, the Trust has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the organisation to:

- run recruitment and promotion processes;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the organisation complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;

- ensure effective general HR and business administration;
- provide references on request for current or former employees; and
- respond to and defend against legal claims.

Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations (such as those in relation to employees with disabilities).

Where the Trust processes other special categories of personal data, such as information about ethnic origin, sexual orientation or religion or belief, this is done for the purposes of equal opportunities monitoring. Data that the Trust uses for these purposes is anonymised or is collected with the express consent of employees, which can be withdrawn at any time. Employees are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so.

**Who has access to data?**

Your information may be shared internally, including with members of the HR and recruitment team (including payroll), your line manager, senior managers and IT staff if access to the data is necessary for performance of their roles.

The Trust shares your data with third parties in order to obtain pre-employment references from other employers, obtain employment background checks from third-party providers and obtain necessary criminal records checks from the Disclosure and Barring Service. In those circumstances the data will be subject to confidentiality arrangements.

The Trust also shares your data with third parties that process data on its behalf:

- Trusts' Choice - in connection with payroll, HR, the provision of benefits and the provision of occupational health services.

- The Department for Education (DfE) - we share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to Trust funding/expenditure and the assessment educational attainment.

The Trust will not transfer your data to countries outside the European Economic Area.

**How does the Trust protect data?**

The Trust takes the security of your data seriously. The Trust has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties. These policies and controls apply to all its constituent Trusts and specialisms.

Where the Trust engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

**For how long does the Trust keep data?**

The Trust will hold your personal data for the duration of your employment.
The periods for which your data is held after the end of employment are set out relevant retention periods.

**Data collection requirements**

The DfE collects and processes personal data relating to those employed by Trusts (including Multi Academy Trusts) and local authorities that work in state funded Trusts (including all maintained Trusts, all academies and free Trusts and all special Trusts including Pupil Referral Units and Alternative Provision). All state funded Trusts are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-Trusts.

The department may share information about Trust employees with third parties who promote the education or well-being of children or the effective deployment of Trust staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to Trust workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact the department: https://www.gov.uk/contact-dfe

**Requesting access to your personal data**

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require the Trust to change incorrect or incomplete data;
- require the Trust to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing; and
- object to the processing of your data where the Trust is relying on its legitimate interests as the legal ground for processing.

If you would like to exercise any of these rights, please contact the Central Administration team:

Email: [insert generic Central Admin team email]
Tel: 01284 761934

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

**What if you do not provide personal data?**

You have some obligations under your employment contract to provide the Trust with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide the Trust with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the Trust to enter a contract of employment with you. If you do not provide other information, this will hinder the Trust's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

**Automated decision-making**
Employment decisions are not based solely on automated decision-making.

**Further information**
If you would like to discuss anything in this privacy notice, please contact:

Joy Griffiths, Central Administration Team, SENDAT

Email: joy.griffiths@sendat.academy
Tel: 01284 722646

**APPENDIX 5**
**SENDAT JOB APPLICANT PRIVACY NOTICE**

As part of any recruitment process, the Trust (including all its constituent Trusts and other specialisms) collects and processes personal data relating to job applicants. The Trust is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

**Who We Are**
Under Data Protection legislation, the Trust is a data controller.

The contact details for the Trust are as follows:
SENDAT, Mount Road, Bury St Edmunds IP32 7BH

**Our Data Protection Officer**
The Trust's data protection officer is currently:
Sian Durrant (Trusts' Choice) – initial contact via the SENDAT Central Administration office.

**What Information Does the Trust Collect?**
The Trust collects a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number;
- details of your qualifications, skills, experience and employment history;
- information about your current level of remuneration, including benefit entitlements;
- whether or not you have a disability for which the Trust needs to make reasonable adjustments during the recruitment process; and
- information about your entitlement to work in the UK.

The Trust may collect this information in a variety of ways. For example, data might be contained in application forms or CVs, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment, including online tests.

The Trust may also collect personal data about you from third parties, such as references supplied by former employers, information from employment background check providers and information from criminal records checks.

Unless you have specifically given your consent for references to be requested before interview, the Trust will seek information from third parties only once a conditional job offer has been made and will inform you that it is doing so.

Data will be stored in a range of different places, including on your application record, in HR management systems and on other IT systems (including email).

**Why does the Trust process personal data?**

The Trust needs to process data to take steps at your request prior to entering into a contract with you. It may also need to process your data to enter into a contract with you.

In some cases, the Trust needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check a successful applicant's eligibility to work in the UK before employment starts.

The Trust has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows the Trust to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. The Trust may also need to process data from job applicants to respond to and defend against legal claims.

The Trust may process special categories of data, such as information about ethnic origin, sexual orientation or religion or belief, to monitor recruitment statistics. It may also collect information about whether or not applicants are disabled to make reasonable adjustments for candidates who have a disability. The Trust processes such information to carry out its obligations and exercise specific rights in relation to employment.

The Trust is obliged to seek information about all its employees with regard to criminal convictions and offences. It does so because it is necessary for it to carry out its obligations and exercise specific rights in relation to employment.

If your application is unsuccessful, the Trust may keep your personal data on file in case there are future employment opportunities for which you may be suited. The Trust will ask for your consent before it keeps your data for this purpose and you are free to withdraw your consent at any time.

**Who Has Access to Data?**

Your information may be shared internally for the purposes of the recruitment exercise. This includes members of the HR and recruitment team, interviewers involved in the recruitment process, managers in the area with a vacancy and IT staff if access to the data is necessary for the performance of their roles.

The Trust will not share your data with third parties, unless you have given your specific consent for references to be sought before interview, or your application for employment is successful and it makes you a conditional offer of employment. The Trust will then share your data with former employers to obtain references for you, employment background check providers to obtain necessary background checks and the Disclosure and Barring Service to obtain necessary criminal records checks.

The Trust will not transfer your data to countries outside the European Economic Area.

**How does the Trust protect data?**

The Trust takes the security of your data seriously. It has internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the proper performance of their duties.

**For How Long Does the Trust Keep Data?**

If your application for employment is unsuccessful, the Trust will hold your data on file for up to three months after the end of the relevant recruitment process. If you agree to allow the Trust to keep your personal data on file, the Trust will hold your data on file for a further 12 months for consideration for future employment opportunities. At the end of that period or once you withdraw your consent, your data is deleted or destroyed.

If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your personnel file and retained during your employment. The periods for which your data will be held will be provided to you in a new privacy notice.

**Your rights**

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require the Trust to change incorrect or incomplete data;
- require the Trust to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing; and
- object to the processing of your data where the Trust is relying on its legitimate interests as the legal ground for processing.

If you would like to exercise any of these rights, please contact:

Joy Griffiths, SENDAT Central Administration Team
Email: joy.griffiths@sendat.academy
Tel: 01284 722646

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

**What if you do not provide personal data?**

You are under no statutory or contractual obligation to provide data to the Trust during the recruitment process. However, if you do not provide the information, the Trust may not be able to process your application properly or at all.

**Automated decision-making**

Recruitment decisions are not based solely on automated decision-making.

**Further information**
If you would like to discuss anything in this privacy notice, please contact:

Joy Griffiths, Central Administration Team, SENDAT

Email: joy.griffiths@sendat.academy
Tel: 01284 722646