



---

# SENDAT

# Data Protection Policy

---

To be reviewed biennially or as required by changes in legislation

Ref:	<b>005-2020</b>
Author:	<b>T Darby</b>
Issued:	<b>March 2020</b>
Reviewed by:	<b>Joy Kent</b>
Changes	<b>Updated to reflect current DPO guidance</b>
Approved by:	<b>Provision Committee at their meeting on: 11.03.2020</b>
Next review:	<b>Spring 2022</b>
Directors:	Received by SENDAT Full Trust Board: 01.04.2020

**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 ..... 7
- 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 ..... 12
- 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 provisions of the Data Protection Act 2018 (DPA 2018) which incorporates the General Data Protection Regulations (GDPR).

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 Data Protection Act 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](#) and the SENDAT Data Protection Officer (provided by Schools' Choice).

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
<b>Personal data</b>	Any information relating to an identified, or identifiable, individual.  This may include the individual's: <ul style="list-style-type: none"><li>• Name (including initials)</li><li>• Identification number</li><li>• Location data</li><li>• Online identifier, such as a username</li></ul> It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
<b>Special categories of personal data</b>	Personal data which is more sensitive and so needs more protection, including information about an individual's: <ul style="list-style-type: none"><li>• Racial or ethnic origin</li><li>• Political opinions</li><li>• Religious or philosophical beliefs</li><li>• Trade union membership</li><li>• Genetics</li><li>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes</li></ul>

	<ul style="list-style-type: none"> <li>• Health – physical or mental</li> <li>• Sex life or sexual orientation</li> </ul>
<b>Processing</b>	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
<b>Data subject</b>	The identified or identifiable individual whose personal data is held or processed.
<b>Data controller</b>	A person or organisation that determines the purposes and the means of processing of personal data.
<b>Data processor</b>	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
<b>Personal data breach</b>	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 schools 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 currently provided by Schools' Choice and the named DPT is Katy Handshaw.

Contact details:

Tel: 01473 260700

Email: [data.protection@schoolschoice.org](mailto:data.protection@schoolschoice.org)

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

Email: [hr@sendat.academy](mailto:hr@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**

SENDAT must comply with Data Protection principles as set out in the Data Protection Act 2018.

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 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 Multi Academy Trusts](#).

## **8. Sharing personal data**

We normally share personal data with third parties only in strict accordance with SENDAT privacy notices (see appendices) but exceptionally may do so in circumstances where:

- There is an issue with a pupil or parent/carers 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 uses CCTV in some of its schools/other provisions to monitor the school premises in order to provide a safe and secure environment for students, staff, visitors and their property. Where CCTV equipment is installed, SENDAT 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 in locations where it is installed, we will 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. See local policies for further information.

### **SENDAT currently uses CCTV at the following Trust locations:**

Chalk Hill Academy

## **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 biennially, or more frequently if there is a change in current, relevant legislation.

### **20. Links with other policies**

This data protection policy is linked to our:

- SENDAT Staff Code of Conduct
- SENDAT Acceptable Use of ICT equipment policy
- SENDAT Confidentiality Policy and Agreement for staff and volunteers
- 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

<b>Name:</b>
<b>Telephone Number:</b>
<b>Email:</b>
<b>Address:</b>
<b>Employee Payroll Number (If relevant):</b>
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.
<b>Required information (and any relevant dates):</b>  <i>Example: Emails between "A" and "B" from 1 May 2017 to 6 September 2017.</i>
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.  Please return this form via email to the Data Protection Officer on <a href="mailto:sian.durrant@Trustschoice.org">sian.durrant@Trustschoice.org</a>  Please allow 1 calendar month for a reply.
<b>Data Subject's Signature:</b>
<b>Date:</b>



## **APPENDIX 3**

### **SENDAT Pupil Privacy Notice (How we use pupil information)**

#### **The categories of personal information that we process include:**

- personal identifiers and contacts (such as name, unique pupil number, contact details and address)
- characteristics (such as ethnicity, language, and free school meal eligibility)
- safeguarding information (such as court orders and professional involvement)
- special educational needs (including the needs and ranking)
- medical and administration (such as doctors information, child health, dental health, allergies, medication and dietary requirements)
- attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- assessment and attainment (such as key stage 1 and phonics results, post 16 courses enrolled for and any relevant results)
- behavioural information (such as exclusions and any relevant alternative provision put in place)

This list is not exhaustive, to access the current list of categories of information we process please contact the school office.

#### **Why we collect and use pupil information**

We collect and use pupil information, for the following purposes:

- a) to support pupil learning
- b) to monitor and report on pupil attainment progress
- c) to provide appropriate pastoral care
- d) to assess the quality of our services
- e) to keep children safe (food allergies, or emergency contact details)
- f) to meet the statutory duties placed upon us for DfE data collections

Under the General Data Protection Regulation (GDPR), the legal bases we rely on for processing personal information are defined under Article 6, and the following sub-paragraphs in the GDPR apply:

- a) Data subject gives consent for one or more specific purposes.
- b) Processing is necessary to comply with the legal obligations of the controller.
- c) Processing is necessary to protect the vital interests of the data subject.
- d) Processing is necessary for tasks in the public interest or exercise of authority vested in the controller (the provision of education).

Our lawful basis for collecting and processing pupil information is also further defined under Article 9, in that some of the information we process is deemed to be sensitive, or special, information and the following sub-paragraphs in the GDPR apply:

- a) The data subject has given explicit consent.

- b) It is necessary to fulfil the obligations of controller or of data subject.
- c) It is necessary to protect the vital interests of the data subject.
- d) Processing is carried out by a foundation or not-for-profit organisation (includes religious, political or philosophical organisations and trade unions)
- e) Reasons of public interest in the area of public health
- f) It is in the public interest

## **Collecting this information**

We collect personal information via data exchange or transition paperwork

Pupil data is essential for the schools' operational use. Whilst the majority of pupil information you provide to us is mandatory, some of it requested on a voluntary basis. In order to comply with the data protection legislation, we will inform you at the point of collection, whether you are required to provide certain pupil information to us or if you have a choice in this.

## **Storing personal data**

We hold pupil data whilst the child remains at Priory School. The file will follow the pupil when they leave Priory School. However where there is a legal obligation to retain the information beyond that period, it will be retained in line with our retention policy.

We have data protection policies and procedures in place, which are regularly reviewed. Further information can be found on our website [www.prioryschool.suffolk.sch.uk](http://www.prioryschool.suffolk.sch.uk)

## **Who we share this information with**

We routinely share pupil information with appropriate third parties, including:

- schools that the pupils attend after leaving us
- our local authority
- youth support services (pupils aged 13+)
- the Department for Education (DfE)
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies

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.

## **Why we share this 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 school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information about Individual Pupils) (England) Regulations 2013.

## **Youth support services**

### **Pupils aged 13+**

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

The information shared is limited to the child's name, address and date of birth. However where a parent or guardian provides their consent, other information relevant to the provision of youth support services will be shared. This right is transferred to the child / pupil once they reach the age 16.

### **Pupils aged 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

Data is securely transferred to the youth support service via data exchange and is stored in accordance to their storage and retention policy.

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

## **The Department for Education**

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our children in need and children looked after with the Department for Education (DfE) for the purpose of those data collections, <https://www.gov.uk/education/data-collection-and-censuses-for-schools>

We share children in need and children looked after data with the Department on a statutory basis, under Section 83 of 1989 Children's Act, Section 7 of the Young People's Act 2008 and also under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current [government security policy framework](#).

For more information, please see 'How Government uses your data' section.

## Requesting access to your personal data

Under data protection legislation, parents, carers and children have the right to request access to information about them that we hold. To make a request for your personal information contact our data protection officer via the school office.

You also have the right to:

- to ask us for access to information about you that we hold
- to have your personal data rectified, if it is inaccurate or incomplete
- to request the deletion or removal of personal data where there is no compelling reason for its continued processing
- to restrict our processing of your personal data (i.e. permitting its storage but no further processing)
- to object to direct marketing (including profiling) and processing for the purposes of scientific/historical research and statistics
- not to be subject to decisions based purely on automated processing where it produces a legal or similarly significant effect on you

If you have a concern or complaint about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at <https://ico.org.uk/concerns/>

For further information on how to request access to personal information held centrally by DfE, please see the 'How Government uses your data' section of this notice.

## Withdrawal of consent and the right to lodge a complaint

Where we are processing your personal data with your consent, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of your personal data, please let us know by contacting our data protection officer; [office@priory.suffolk.sch.uk](mailto:office@priory.suffolk.sch.uk)

## Last updated

We may need to update this privacy notice periodically so we recommend that you revisit this information from time to time.

## Contact

If you would like to discuss anything in this privacy notice, please contact Data Protection Officer via [hr@sendat.academy](mailto:hr@sendat.academy), or talk to your local Headteacher/Head of School via the school office.

## How Government uses your data

The data that we lawfully share with the DfE through data collections helps to:

- develop national policies
- manage local authority performance

- administer and allocate funding
- identify and encourage good practice

## Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education go to:

Children in need: <https://www.gov.uk/guidance/children-in-need-census>

Children looked after: <https://www.gov.uk/guidance/children-looked-after-return>

## The National Pupil Database (NPD)

Much of the data about pupils in England goes on to be held in the National Pupil Database (NPD).

The NPD is owned and managed by the Department for Education and contains information about pupils in schools 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 schools, local authorities and awarding bodies.

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

## Sharing by the Department

The law allows the department to share pupils' personal data with certain third parties, including:

- schools and local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

For more information about the department's NPD data sharing process, please visit:

<https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

Organisations fighting or identifying crime may use their legal powers to contact DfE to request access to individual level information relevant to detecting that crime. Whilst numbers fluctuate slightly over time, DfE typically supplies data on around 600 pupils per year to the Home Office and roughly 1 per year to the Police.

For information about which organisations the department has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website: <https://www.gov.uk/government/publications/dfе-external-data-shares>

## How to find out what personal information DfE hold about you

Under the terms of the Data Protection Act 2018, you're entitled to ask the Department:

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department, you should make a 'subject access request'. Further information on how to do this can be found within the Department's personal information charter that is published at the address below:

<https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter>

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

## **SENDAT Pupil Privacy Notice (How we use children in need and children looked after information)**

### **The categories of personal information that we process include:**

- personal information (such as name, date of birth and address)
- characteristics (such as gender, ethnicity and disability)
- episodes of being a child in need (such as referral information, assessment information, Section 47 information, Initial Child Protection information and Child Protection Plan information)
- episodes of being looked after (such as important dates, information on placements)
- outcomes for looked after children (such as whether health and dental assessments are up to date, strengths and difficulties questionnaire scores and offending)
- adoptions (such as dates of key court orders and decisions)
- care leavers (such as their activity and what type of accommodation they have)

This list is not exhaustive, to access the current list of categories of information we process please contact the school office.

### **Why we collect and use this information**

We use this personal data to:

- a) support these children and monitor their progress
- b) provide them with pastoral care
- c) assess the quality of our services
- d) evaluate and improve our policies on children's social care

Under the General Data Protection Regulation (GDPR), the legal bases we rely on for processing personal information are defined under Article 6, and the following sub-paragraphs in the GDPR apply:

- a) Data subject gives consent for one or more specific purposes.
- b) Processing is necessary to comply with the legal obligations of the controller.
- c) Processing is necessary to protect the vital interests of the data subject.
- d) Processing is necessary for tasks in the public interest or exercise of authority vested in the controller (the provision of education).

Our lawful basis for collecting and processing pupil information is also further defined under Article 9, in that some of the information we process is deemed to be sensitive, or special, information and the following sub-paragraphs in the GDPR apply:

- a) The data subject has given explicit consent.
- b) It is necessary to fulfil the obligations of controller or of data subject.
- c) It is necessary to protect the vital interests of the data subject.
- d) Processing is carried out by a foundation or not-for-profit organisation (includes religious, political or philosophical organisations and trade unions)
- e) Reasons of public interest in the area of public health

- f) It is in the public interest

### **Collecting this information**

We collect personal information via data exchange or transition paperwork

Children in need and children looked after information is essential for the local authority's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it requested on a voluntary basis. In order to comply with GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

### **Storing personal data**

We hold pupil data whilst the child remains at Priory School. The file will follow the pupil when they leave Priory School. However where there is a legal obligation to retain the information beyond that period, it will be retained in line with our retention policy.

We have data protection policies and procedures in place, which are regularly reviewed. Further information can be found on our website [www.prioryschool.suffolk.sch.uk](http://www.prioryschool.suffolk.sch.uk)

### **Who we share this information with**

We routinely share pupil information with appropriate third parties, including:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions
- The Department for Education
- The pupil's family and representatives
- Educators and examining bodies
- Ofsted
- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies
- Schools that the pupil's attend after leaving us

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.



## Why we share this information

We do not share information about our children in need or children looked after 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 school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information about Individual Pupils) (England) Regulations 2013.

## The Department for Education

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our children in need and children looked after with the Department for Education (DfE) for the purpose of those data collections, <https://www.gov.uk/education/data-collection-and-censuses-for-schools>

We share children in need and children looked after data with the Department on a statutory basis, under Section 83 of 1989 Children's Act, Section 7 of the Young People's Act 2008 and also under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current [government security policy framework](#).

For more information, please see 'How Government uses your data' section.

## Requesting access to your personal data

Under data protection legislation, parents, carers and children have the right to request access to information about them that we hold. To make a request for your personal information contact our data protection officer via the school office.

You also have the right to:

- to ask us for access to information about you that we hold
- to have your personal data rectified, if it is inaccurate or incomplete
- to request the deletion or removal of personal data where there is no compelling reason for its continued processing
- to restrict our processing of your personal data (i.e. permitting its storage but no further processing)
- to object to direct marketing (including profiling) and processing for the purposes of scientific/historical research and statistics
- not to be subject to decisions based purely on automated processing where it produces a legal or similarly significant effect on you

If you have a concern or complaint about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at <https://ico.org.uk/concerns/>

For further information on how to request access to personal information held centrally by DfE, please see the 'How Government uses your data' section of this notice.

### **Withdrawal of consent and the right to lodge a complaint**

Where we are processing your personal data with your consent, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of your personal data, please let us know by contacting our data protection officer; [office@priory.suffolk.sch.uk](mailto:office@priory.suffolk.sch.uk)

### **Last updated**

We may need to update this privacy notice periodically so we recommend that you revisit this information from time to time.

### **Contact**

If you would like to discuss anything in this privacy notice, please contact Data Protection Officer via [hr@sendat.academy](mailto:hr@sendat.academy), or talk to your local Headteacher/Head of School via the school office.

### **How Government uses your data**

The data that we lawfully share with the DfE through data collections helps to:

- develop national policies
- manage local authority performance
- administer and allocate funding
- identify and encourage good practice

### **Data collection requirements**

To find out more about the data collection requirements placed on us by the Department for Education go to:

Children in need: <https://www.gov.uk/guidance/children-in-need-census>

Children looked after: <https://www.gov.uk/guidance/children-looked-after-return>

### **The National Pupil Database (NPD)**

Much of the data about pupils in England goes on to be held in the National Pupil Database (NPD).

The NPD is owned and managed by the Department for Education and contains information about pupils in schools 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 schools, local authorities and awarding bodies.

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

## Sharing by the Department

The law allows the department to share pupils' personal data with certain third parties, including:

- schools and local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

For more information about the department's NPD data sharing process, please visit:

<https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

Organisations fighting or identifying crime may use their legal powers to contact DfE to request access to individual level information relevant to detecting that crime. Whilst numbers fluctuate slightly over time, DfE typically supplies data on around 600 pupils per year to the Home Office and roughly 1 per year to the Police.

For information about which organisations the department has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website: <https://www.gov.uk/government/publications/dfе-external-data-shares>

## How to find out what personal information DfE hold about you

Under the terms of the Data Protection Act 2018, you're entitled to ask the Department:

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department, you should make a 'subject access request'. Further information on how to do this can be found within the Department's personal information charter that is published at the address below:

<https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter>

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

## **APPENDIX 4**

### **SENDAT STAFF PRIVACY 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**

Our Data Protection Officer is currently provided by Schools' Choice and the named DPT is Katy Handshaw.

Contact details:

Tel: 01473 260700

Email: [data.protection@schoolschoice.org](mailto:data.protection@schoolschoice.org)

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

Email: [hr@sendat.academy](mailto:hr@sendat.academy)

Tel: 01284 761394

#### **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, SENDAT Directors 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:

- Schools' 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: [hr@sendat.academy](mailto:hr@sendat.academy)

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 the SENDAT HR Manager (currently Joy Kent).

Email: [hr@sendat.academy](mailto:hr@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**

Our Data Protection Officer is currently provided by Schools' Choice and the named DPT is Katy Handshaw.

Contact details:

Tel: 01473 260700

Email: [data.protection@schoolschoice.org](mailto:data.protection@schoolschoice.org)

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

Email: [hr@sendat.academy](mailto:hr@sendat.academy)

Tel: 01284 761394

#### **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](mailto: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 the SENDAT HR Manager (currently Joy Kent).

Email: [hr@sendat.academy](mailto:hr@sendat.academy)

Tel: 01284 722646