



# Bright Futures

EDUCATIONAL TRUST

The best *for* everyone, the best *from* everyone

## Data Privacy Policy Pupils, parents/carers

This is a Trust-Wide Policy  
which applies to all the schools within the Trust

Date of Policy Approval:

Sept 2023

Owner of Policy:

Data Protection  
Officer

Authorised By:

Board of  
Trustees

Policy Review Date:

Autumn 2025

Distribution:

**All staff,  
workers,  
governors and  
trustees**

**Website**

## CONTENTS

<b>PUPILS, PARENTS AND CARERS DATA SECURITY POLICY</b>	<b>4</b>
<b>DATA PRIVACY POLICY - EDUCATION</b>	<b>4</b>
<b>What is the Policy for?</b>	<b>4</b>
<b>Who is the Policy for?</b>	<b>4</b>
<b>About this policy</b>	<b>4</b>
<b>Definitions</b>	<b>5</b>
<b>Policy Standards</b>	<b>6</b>
<b>1. Data protection and educational records</b>	<b>6</b>
<b>2. Fair, lawful and transparent processing</b>	<b>6</b>
<b>3. How the Trust is likely to use personal data</b>	<b>7</b>
Publishing Student’s Images and Work	<b>7</b>
Storage of Images	<b>8</b>
Webcams	<b>8</b>
Use of Biometric Data	<b>9</b>
Special Category Personal Data	<b>9</b>
<b>4. Processing for specified, explicit and legitimate purposes</b>	<b>10</b>
<b>5. Adequate, relevant and limited to what is necessary</b>	<b>10</b>
<b>6. Accurate and when necessary, kept up to date</b>	<b>10</b>
<b>7. Data retention</b>	<b>10</b>
<b>8. Data security</b>	<b>10</b>
<b>9. Sharing information with third parties</b>	<b>11</b>
<b>10. Processing in line with subject access rights</b>	<b>13</b>
<b>11. Subject access requests</b>	<b>14</b>
<b>12. Data Protection Officer (“DPO”)</b>	<b>15</b>
<b>13. Breaches of data protection and complaints</b>	<b>16</b>
<b>14. CONSENT</b>	<b>17</b>
<b>15. LAST UPDATED</b>	<b>17</b>
<b>Addendum 1- Personal Data Retention periods- Pupils, parents/carers Personal Data types held by the Trust/Local Governing Body/Principal and senior leadership team in academies</b>	<b>18</b>

## DATA PRIVACY POLICY PUPILS, PARENTS AND CARERS DATA SECURITY POLICY

### DATA PRIVACY POLICY - EDUCATION

Bright Futures Educational Trust's Strategy underpins all aspects of this policy and the way in which it will be applied. These elements are:

- Our vision, the best **for** everyone, the best **from** everyone;
- Two of our values; **Integrity**: We do the right things for the right reasons and **Passion**: We take responsibility, work hard and have high aspirations;
- Two of our commitments: **Effective Communication** and **Strong Governance and Accountability**.

### What is the Policy for?

This policy sets out the duties of Bright Futures Educational Trust ("the **Trust**") under General Data Protection Regulation ("GDPR"), the Data Protection Act 2018, and is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department for Education. The policy details the responsible bodies/person for compliance and the procedures that will be applied.

By Trust we mean, all academies in the Trust and the head office of the Trust.

### Who is the Policy for?

Part Two of this policy is for pupils and parents/cares to understand how their personal data will be handled. It is also for staff to understand their responsibilities in handling the personal data of pupils, parents and carers. It is published on our website.

Part One of this policy is for the attention of anyone who is employed by, provides a service to, or volunteers to work at the Trust and its academies. This includes governors and trustees.

### About this policy

Our Trust processes personal information relating to pupils, staff and visitors, and, therefore, is a Controller.

The Trust is registered as a Controller with the Information Commissioner's Office and renews this registration annually. The Trust's registration number is: ZA023935.

During the course of its activities the Trust will process personal data (which may be held on paper, electronically, or otherwise) about the Trust's staff (including temporary staff), agency workers, volunteers, pupils, their parents, or carers, and other individuals (including suppliers and governors and trustees).

The Trust Board also complies with ICO and DfE Guidance applicable from time to time.

## Definitions

The definitions in this paragraph apply in this policy.

Term	Definition
<b>Personal data</b>	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identifiable
<b>Special categories of personal data (formerly sensitive)</b>	Data such as: <ul style="list-style-type: none"> <li>• Racial or ethnic origin</li> <li>• Political opinions</li> <li>• Religious beliefs, or beliefs of a similar nature</li> <li>• Where a person is a member of a trade union</li> <li>• Physical and mental health</li> <li>• Sexual orientation and sex life</li> <li>• Biometric or genetic data</li> </ul>
<b>Criminal conviction data</b>	Data relating to criminal convictions and offences (this includes unproven allegations, information relating to the absence of convictions and data relating to alleged and actual victims, along with witnesses of crime).
<b>Processing</b>	This has a very wide definition and includes the following operations with personal data: collection, recording, organisation, structuring, storage, adaption, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure and/or destruction.
<b>Data subject</b>	The living individual whose personal data is held or processed

<b>Controller</b>	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
<b>Processor</b>	A person or organisation that processes personal data on behalf of a Controller.

## Policy Standards

### 1. Data protection and educational records

The Trust will comply with the six data protection principles in the GDPR, which require that personal data must be:

- processed lawfully, fairly and in a transparent manner.
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- adequate, relevant and limited to what is necessary in relation to the purpose for which it is maintained.
- accurate and, where necessary, kept up to date.
- not be kept in a form which permits identification for longer than is necessary for the purpose(s) for which it is processed; and
- processed in a manner that ensures appropriate security of the data.

### 2. Fair, lawful and transparent processing

- The Trust will only process personal data where it is based one or more of the conditions specified in the GDPR. The most common conditions we rely on to process personal data are:

<b>Conditions for Processing which we commonly rely on</b>	
<b>Personal Data</b>	<b>Special Category Personal Data &amp; Criminal Convictions Data</b>
<ul style="list-style-type: none"> <li>• The data subject has given consent to the processing for one or more specific purposes.</li> <li>• Processing is necessary for entering or performing a contract with the data subject.</li> <li>• Processing is necessary for compliance with a legal obligation to which the controller is subject.</li> <li>• Processing is necessary to protect the vital interests of the data subject.</li> <li>• Processing is necessary in order for the controller to perform a task in the public interest or for the controller's official</li> </ul>	<ul style="list-style-type: none"> <li>• The data subject has given explicit consent to the processing for one or more specific purposes.</li> <li>• Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.</li> </ul>

<p>functions, and the task or function has a clear basis in law; or</p> <ul style="list-style-type: none"> <li>• Processing is necessary for the purposes of legitimate interests pursued by the data controller or by a third party where this does not relate to our “core function” of providing education.</li> </ul>	<ul style="list-style-type: none"> <li>• Processing is necessary to protect the vital interests of the data subject or of another natural person, where the data subject is physically or legally incapable of giving consent.</li> <li>• Processing relates to personal data which are manifestly made public by the data subject.</li> <li>• Processing is necessary for reasons of substantial public interest.</li> <li>• Processing is necessary for the establishment, exercise or defence of legal claims; or</li> <li>• Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services (however this condition is limited in its use to certain authorised professions as explained at Article 9(3) GDPR).</li> </ul>
---	--

- The full list of conditions is set out in Articles 6 and 9 of the GDPR and the Trust may in some circumstances rely on other conditions set out in the GDPR or Data Protection Act 2018 to justify the processing of personal data or special category personal data. The ICO’s website also has further information about the lawful conditions for processing.

### 3. How the Trust is likely to use personal data.

The Trust will process the following categories of **pupil** information:

- 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)

The Trust will process data about **pupils** for the following (non-exhaustive) purposes:

- for legal and administrative purposes;
- to provide education and discharge the **Trust's** duty of care as an education provider;
- to provide pupils with a safe and secure environment and pastoral care;
- to provide activities including school trips, activity and after-school clubs;
- to support pupil learning;
- to monitor and report on pupil progress;
- to provide academic and examination references;
- to enable the **Trust** to meet its legal obligations under relevant legislation and Department for Education (DfE) Guidance in force from time to time;
- to assess the quality of the Trust's services;
- to maintain educational records;
- to monitor attendance;
- to maintain health and safety records;
- to collect opinions about ability and achievements;
- to obtain and retain details about personal / home life where this is relevant to provision of education to a data subject; and,
- to share information with other agencies when required including for Department for Education data collections.

Under the UK General Data Protection Regulation (UK GDPR), the lawful bases the Trust relies on for processing pupil information are:

- for the purpose of delivering pupil education in accordance with the legal basis of performing a task in the public interest.
- to meet a legal obligation placed on the school to collect information on attendance, admissions and other areas as prescribed by law.
- in the vital interests of pupils or parents to ensure that the Trust can react speedily in certain circumstances that require immediate responses.
- to obtain consent when the Trust uses images of pupils on its website, in its prospective or through social media channels that it maintains.

In addition, concerning any special category data:

- when there is a substantial public interest to share information with a multi-disciplinary team to protect the welfare of a pupil
- when the Trust has explicit consent to process biometric data for cashless catering services
- when the Trust is establishing or defending its legal rights.

The Trust collects pupil information via registration forms/data collection forms at the start of each academic year and/or Common Transfer File (CTF) from previous schools for transfers.

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.



### 3.1. Publishing Student's Images and Work

On a student's entry to the academy, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- On the school website, or social media feeds.
- In the academy prospectus and other printed publications that the academy or Trust may produce for promotional purposes.
- Recorded/ transmitted on a video or webcam.
- In display material that may be used in the academy's communal areas.
- In display material that may be used in external areas, i.e. exhibition promoting the academy.
- General media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

Parents/ carers may withdraw permission, in writing, at any time, or by other means provided by the academy (e.g. using the Data Collection system in SLG). We request consent to be given by the resident parent/carers for it to be deemed valid. From the age of 12, if a pupil has the ability to understand the nature of the request and what the consequences of providing it will be, the Trust will seek permission. When obtaining consent, we will set out that we wish to use a child's images for the duration of their time with us and for 6 years after they have left.

Pupils' full names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published.

Where pupils' full names are to be published (e.g. to celebrate examination results), parents/carers will be given opportunity to opt out.

Before posting student work on the Internet, staff will check that permission has been given for work to be displayed from an up-to-date list.

### 3.2. Storage of Images

- Images / films of children are stored on the Trust/school's secure network.
- CCTV is used for security purposes. We do not seek consent for the use of CCTV images as these are collected in accordance with our public task to keep children in our care safe. Access to CCTV footage is limited to those staff/governors whose roles require it.
- Rights of access to this material are restricted to the staff and pupils within the confines of the school network, or via secure Remote Desktop connections.
- Images and videos of pupils recorded or stored on equipment (e.g. trips, mementoes of previous classes) will be in line with appropriate legislation and the Teachers' Standards.
- The IRIS system may be used to record lessons for staff appraisal and reflection. Since the videos are stored in an encrypted form, cannot be downloaded and may only be shared with other staff at school, explicit permission need not be sought (similar to CCTV).

### 3.3. Webcams

- Webcams in school are only ever used for specific learning purposes, e.g. monitoring science experiments such as eggs hatching or video conferencing.
- Misuse of the webcam by any member of the community will result in investigation and sanctions.
- Consent for publication of images extends to use of webcams.

### 3.4. Use of Biometric Data

Any biometric information (defined as: “*personal information about an individual’s physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements*”) must be stored in accordance with Data Protection legislation.

The Trust uses biometric data in its academies for a cashless payment system. In accordance with the Protections of Freedoms Act 2012 the Trust will obtain parental consent for all pupils up to the age of 18. All pupils are also entitled to refuse to have their fingerprint used for this system regardless of whether a parent consents. If that is the case, alternative payment methods for our cashless catering services will be used.

### 3.5. Special Category Personal Data

**The Trust may process special category personal data relating to pupils** including, as appropriate:

- information about pupil’s physical or mental health or condition (including but not limited to allergies and regular medications) in order to discharge the **Trust’s** duty of care, provide non-emergency and emergency medical assistance and for special educational needs provision;
- provide applicable provision under an Education Health and Care Plan/Statement of Special Educational Needs;
- the pupil’s racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation or to ensure that religious or similar beliefs are respected;
- share in a multi-professional team around a child; and/or,
- in order to comply with other legal requirements and obligations to third parties.

**The Trust may process data about parents, carers and other individuals** for the purpose of:

- providing education to pupils;
- reporting on pupil progress;
- maintaining emergency contact details in order to discharge the Trust’s duty of care as an education provider;
- organise training courses;
- obtain and retain details about personal / home life where this is relevant to provision of education to pupils; and
- discharge obligations under safeguarding and other relevant legislation.

- It is very unlikely that the Trust will process sensitive personal data relating to parents, carers and other individuals . However, where this may be necessary, it may include, as appropriate:
- the parent, carer or other individual’s racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
- when there is relevant medical information needed for health and safety purposes including allergy information; and/or,
- in order to comply with other legal requirements and obligations to third parties.

#### **4. Processing for specified, explicit and legitimate purposes**

- The Trust will only process personal data for the specific, explicit and legitimate purpose or purposes notified to data subjects and will not be further processed in any manner incompatible with that purpose or purposes.

#### **5. Adequate, relevant and limited to what is necessary**

- Personal data will only be processed to the extent that it is relevant and necessary for the specific purposes notified to the data subject.

#### **6. Accurate and when necessary, kept up to date**

- The Trust will keep the personal data the Trust stores about a data subject accurate and when necessary, kept up to date. Data that is inaccurate or out of date will be corrected or deleted without delay. Data subjects should notify the Trust if any personal details change or if the data subject becomes aware of any inaccuracies in the personal data the Trust hold about him/her.

#### **7. Data retention**

- The Trust will not keep personal data for longer than is necessary for the purpose for which it is processed. Sometimes we are required by law to retain information for a specified period. After the retention period has lapsed, and there is no other legitimate reason to retain the information, the Trust will take steps to destroy it so that it is no longer processing it.
- The table in Addendum 1 specifies the retention period of personal data relating to pupils, parents, carers and other individuals (including suppliers, governors and trustees). Retention periods for staff/workers’ data is contained in the Data Privacy Policy-Staff.

#### **8. Data security**

The Trust will ensure that appropriate measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

Appropriate measures include:

- Appropriate levels of authority being given to staff members where access to personal data is required;
- Personal data is stored on the academy’s central computer system instead of individual PCs, laptops, tablet devices, mobile telephones etc;
- Computers and laptops are not left unattended without locking their screens via password controls to prevent unauthorised access;

- Personal Data is not carried off-site, unless it is on permitted storage devices which are encrypted and password protected or when it is legally necessary to do so. Where Personal Data needs to be carried off-site in paper form, staff must follow any guidance issued from time to time to ensure the information is kept safe and secure to avoid any personal data breaches.

**Our key security procedures are as follows:**

- Lockable cabinets, drawers and cupboards;
- Lockable offices
- Clear desk policy when leaving a desk or leaving the office for the day, unless it is locked, and no access can be gained by other staff including cleaners
- Laptop and other mobile device / document encryption;
- Laptop and other mobile device / document password protection;
- Regular back-ups of the Academy/Trust's servers;
- Sharing personal data internally (i.e. from person to person in the academy/trust is only done in accordance with the Data protection Principles in Section 1 above)
- Where personal data is shared by email, whenever practicable, it will be attached to the email as an encrypted document.
- ICT Acceptable Use Agreements are signed by all staff/Governors/Pupils/Visitors who will use the school's IT Systems. See our E-Safety policy.
- Servers are kept in rooms which are only accessed by DBS-checked staff.
- Backups are stored securely offsite or in approved, cloud hosted storage and subject to contractual agreements to ensure information provided is processed in a secure and legally compliant way.
- We use recommended disposal firms to securely destroy drives where personal data may have been stored.
- Papers are shredded for secure disposal
- Disks are overwritten or physically destroyed prior to recycling where they may have been used for storing personal data.

**9. Sharing information with third parties**

- The Trust has in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. The Trust will only transfer personal data to a third party the third party agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.
- Where the Trust uses a third-party processor to process personal data on its behalf, it will have in place a written agreement with each processor which meets the requirements of Article 28 of the UK GDPR.
- The **Trust** routinely shares pupil information with:
  - schools that the pupil attends after leaving us;
  - our local authority/councils
  - social services/ children's services where there are safeguarding concerns;
  - the Department for Education (DfE);

- any appointed processor, who analyses pupil data on our behalf to provide academy and trust wide management information.
  - Feeder schools
- 
- The Trust does not share information about pupils with anyone without consent unless the law and our policies allow us to do so.
  - The Trust will share information with multiple agencies which are formed as a team around a child or young person. These agencies will be controllers and be subject to the same obligations under data protection law as the Trust is. The Trust will be under a legal obligation to share most of the information that is relevant to the multi-agency team or will be required to do so in the performance of the school's public task.
  - The Trust is also legally required to pass certain information about pupils to specified external bodies, such as our local authority and the Department for Education (DfE), so that they are able to meet their statutory obligations. This data sharing underpins school funding and educational attainment policy and monitoring.

### **Department for Education**

- The Department for Education collects personal data from educational settings and local authorities via various statutory data collections. The Trust is required to share information about our pupils with the DfE either directly or via our local authority under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.
- All data is transferred securely and held by the Department for Education (DfE) under a combination of software and hardware controls, which meet the current government security policy framework.

### **Pupils aged 13+**

- Once pupils reach the age of 13, the Trust also passes 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 14 Education and Skills Act 2008 (to enable the local authority to meet the requirements of 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+

- The Trust 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 and how personal information will be used for these, please visit the relevant local authority website.
- The Trust will only transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:
  - The country ensures an adequate level of protection for the individuals' rights and freedoms;
  - The individual has given consent;
  - The transfer is necessary for one of the conditions set out in the GDPR (e.g. for the performance of a contract between us and the individual, or to protect the vital interests of the individual);
  - The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims; or
  - The transfer is authorised by the Information Commissioner where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights

## 10. Processing in line with subject access rights

Individuals have the rights when it comes to how we handle their personal data. Some of these rights are dependent on the nature and purpose of the processing. The rights can be exercised by contacting the Trust's DPO (whose details are at the end of this policy).

Right	What it is for?
To be informed	This policy and any accompanying privacy notice sets out the information about how the Trust processes personal data about pupils and parents. It will be reviewed annually to ensure we are as transparent as possible about the personal data that we process.
Rectification	If the Trust is processing an inaccurate record about an individual they have the right to request that we review it and rectify it so as to make it accurate. This only extends to factual information being processed about an individual.
Erasure	If the Trust has no compelling reason to process data about an individual, there is a right for the

	<p>data to be erased and processed no further. This is not an absolute right and the Trust will consider requests on a case by case basis.</p>
Restrict processing	<p>This right complements the right to rectification. Processing of personal data can be restricted whilst the Trust considers if any records are inaccurate or an objection has been raised about the personal data that it is processing.</p>
Data portability	<p>This enables individuals to seek (in certain circumstances) for information which they have provided to the Trust and which is being processed through automated means based on their consent or for the performance of a contract to have it transmitted in machine readable form to the individual or a third party.</p> <p>It is unlikely that this right will apply to the information which the Trust processes about parents and pupils. It could extend to images processed by the Trust when the lawful condition relied upon is consent.</p>
To object	<p>When the Trust is processing personal data about pupil's and parents for the performance of a task in the public interest those individuals have the right to object to processing. The Trust will consider any objection but may be able to demonstrate a legitimate ground to continue to process the personal data concerned.</p>
To know about any automated decision making and profiling	<p>The Trust will inform individuals when it uses any automated decision making processes. Individuals are entitled to request that automated decisions involving them are reviewed by human intervention.</p> <p>We profile pupils' performance to ensure that the school can meet their educational needs.</p>

### 11. Subject access requests

- Under the data protection law, individuals have a right to request access to information the Trust holds about them. This is known as a subject access request. For our Secondary schools this means for a parent to make a subject access request on behalf of a pupils, the pupil must be under 12 or aged 12 and over (subject to the child having sufficient understanding) and having given their consent.

For our Primary/early years' establishments, parents can exercise a pupil's right of access on their behalf due to their age and lack of understanding of the rights afforded over their personal information.

For those pupils with special educational needs we will need to consider their level of competency to consider if they are able to exercise their data subject rights on their own behalf, or if their parent or carer must do this.

- Requests can be made orally or in writing should include:
  - The pupil's name
  - A correspondence address
  - A contact number and email address
  - Details about the information requested to assist the school to confirm if the personal data is being processed and to provide a copy within the time period afforded

**Where access to data is verbally requested, the school or Data Protection Officer will confirm the exact request in writing, in order to ensure the accuracy of the request.**

- The Trust will not reveal the following information in response to subject access requests:
  - Information that might cause serious harm to the physical or mental health of the pupil or another individual
  - Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
  - Information contained in adoption and parental order records
  - Certain information given to a court in proceedings concerning the child
  - Third party personal data where there is no consent to disclose this in response to a subject access request and it would not be reasonable in the circumstances to do so.
- Once the identity of the requestor is verified, the information will generally be provided within 30 calendar days. If the request is complex or numerous the Trust has the right to determine that up to a further 2 months is required to respond to a subject access request. The DPO will write to the data subject within a month of their written request to set out the reasons why the time is being extended.
- If the request is determined to be manifestly unfounded or excessive, the Trust has the right to either charge a fee to reflect the administrative costs of providing the response or to refuse to provide a response. In the event that such a determination is made, the DPO will write to set out the Trust's reasons within a month of the written request being made.

## 12. Data Protection Officer ("DPO")

The **Trust** has appointed a Data Protection Officer who has overall responsibility for the **Trust's** policies and procedures relating to data privacy. The Data Protection Officer should be the first point of contact for individuals in the following situations:

Where individuals have any concerns, or require clarification, about the **Trust's** obligations regarding data privacy and how we handle data;

- To report a data breach or potential data breach;



- Where an individual has any feedback or suggestions about how the **Trust** can improve its data privacy and/or security procedures;
- Where an individual wishes to make a subject access request or exercise one of their other data privacy rights.

Our Data Protection Officer is: Anna Sharpley

Her contact details are:

Telephone: 0161 941 5681. Email: [dataprotection@bright-futures.co.uk](mailto:dataprotection@bright-futures.co.uk).

Postal: The Hub, 144 Irlam Road, Flixton, Manchester, M41 6NA

### **13. Breaches of data protection and complaints**

- If an individual considers that this policy has not been followed in respect of personal data about a data subject he/she should raise the matter with the Data Protection Officer in the first instance.
- Compliance with data protection law is regulated by the Information Commissioner. In the event that you are not satisfied with the way in which the Trust is processing your personal data and you are not content with the response from our DPO, you have the right to refer your concerns to the Information Commissioner's Office ("ICO"). You can contact the ICO at <https://ico.org.uk/concerns/> or via its helpline number which is available on its website.

### **14. CONSENT**

Where the Trust processes personal data with consent, the individual has the right to withdraw that consent. If you change your mind, or are unhappy with our use of your personal data, please contact the DPO.

### **15. LAST UPDATED**

We may need to update this privacy policy periodically, so we recommend you revisit this information from time to time. This version was last updated on 29/08/2023.

**Addendum 1- Personal Data Retention periods. Personal Data types for pupils, parents/carers held by the Trust/Local Governing Body/Principal and senior leadership team in academies**

Basic description	Statutory Provisions that may apply	Retention period	Action at the end of the retention period
Papers and minutes that contain reference to named pupils or parents/carers	Education Act 2002, section 3.3  Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002 S1 2002 No 1171	6 years, with a review of the personal data held after 3 years	Secure disposal
Admissions	School Admissions Code Statutory Guidance for admission authorities, governing bodies, local authorities, schools adjudicators and appeals panels September 2021	Data of admission/decline/resolution of an appeal + 1 year	Secure disposal
Admissions register	Working Together to Improve School Attendance, May 2022	Permanently	Not applicable
Pupil's educational record and file – primary (including internal and external examination results)	The Education (Pupil Information) (England) Regulations 2005 S1 No 1437	Whilst the child is in school	The file is then transferred when the pupil moves to another primary school/secondary/pupil referral unit. In the case of a pupil death, transfer to an independent school, transfers to home schooling or leaves the country; file is transferred to the Local Authority to be retained in accordance with their policy.
Pupil's educational record and file – secondary (including internal and external examination results)	The Education (Pupil Information) (England) Regulations 2005 S1 No 1437  Limitation Act 1980 (Section 2)	Until the child is 25 years of age	Secure disposal  All uncollected examination certificates should be returned to the examination board

Basic description	Statutory Provisions that may apply	Retention period	Action at the end of the retention period
Child Protection information held on pupil file	<p>“Keeping Children Safe in Education September 2022”- Statutory Guidance, as updated from time to time</p> <p>“Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children –March 2015” and as updated from time to time</p>	Retained for the period of the pupil file, in a sealed envelope	Secure disposal, and must be shredded
Child Protection information held in separate files	<p>Keeping Children Safe in Education- Statutory Guidance, as updated from time to time</p> <p>“Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children –July 2018” and as updated from time to time</p>	Until the child is 25 years of age.	Secure disposal, and must be shredded
Accident Reports		Until the child is 25 years of age	Secure disposal
CCTV images	<p>Information Commissioners’ Office (ICO) Code of Practice: <a href="https://ico.org.uk/media/1542/cctv-code-of-practice.pdf">https://ico.org.uk/media/1542/cctv-code-of-practice.pdf</a></p>	30 days, or longer if the footage is needed for a particular matter such as an incident of pupil behaviour	Secure disposal
Student grant/bursaries information		6 years	Secure disposal
Pupil premium/free school meals		6 years	Secure disposal
Attendance registers	Working Together to Improve School Attendance, May 2022	3 years from the date of the entry	Secure disposal
Correspondence relating to authorised absence	Education Act 1996 Section 7	Current academic year +2 years	Secure disposal
Special Educational Needs files, reviews and individual education plans	Limitation Act 1980 (Section 2)	Until the child is 25 years of age	Secure disposal
Statement maintained under Section 234 of the Education Act 1990 and any amendments made to the statement	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	Until the child is 25 <i>years of age</i> (usually held as part of the pupil file)	Secure disposal unless the document is subject to legal hold

<b>Basic description</b>	<b>Statutory Provisions that may apply</b>	<b>Retention period</b>	<b>Action at the end of the retention period</b>
Advice and information provided to parents regarding educational needs	Special Educational Needs and Disability Act 2001 Section 2	Until the child is 25 years of age (usually held as part of the pupil file)	Secure disposal unless the document is subject to legal hold
Accessibility Strategy	Special Educational Needs and Disability Act 2001 Section 14	Until the child is 25 years of age (usually held as part of the pupil file)	Secure disposal unless the document is subject to legal hold
Parental consent forms for school trips where there has been no major incident		Conclusion of the trip	Secure disposal
Parental consent forms for school trips where there has been a major incident	Limitation Act 1980 (Section 2)	Until the child is 25 years of age (to show that rules had been followed)	Secure disposal
Visitors Books and signing in sheets		6 years	Secure disposal