Unique Policy Number: 23

Data Protection and Records Management Policy

The Children's Endeavour Trust comprises:

Abbot's Hall Community Primary School
Bosmere Community Primary School
Broke Hall Community Primary School
Chilton Community Primary School
Combs Ford Primary School
Freeman Community Primary School
Springfield Junior School
Whitehouse Community Primary School

Document Control

Version	*Date*	*Author*	*Comments*
Issue 1	**Feb 2020**	**CEO**	
	March 2022	**CEO**	References to Information and Records Management Society's toolkit added.
	March 2024	**KW**	
	March 2026	**KW**	Added Artificial Intelligence section and updated legislation.

Owner: DPO
Approver: Trust Board
Statutory Policy: Yes
Review Cycle: 2 years
Approval date: 26th March 2026

Policy Contents

1. Introduction and Aims

The Children's Endeavour Trust and its schools (collectively referred as "CET" or "Trust") is committed to protecting the rights and freedom of all individuals in relation to the processing of their data.

This policy will be updated as necessary to reflect best practice, case law, or amendments made to data protection legislation, and shall be reviewed biannually

CET aims to ensure that all data collected about staff, pupils, parents, governors, trustees, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

This policy applies to all personal data, regardless of whether it is paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020

- Data Protection Act 2018 (DPA 2018)

- Guidance published by the Information commissioner's Office (ICO) reflects the GDPR and code of practice for the use of surveillance camera and personal information.

- It meets requirements of the Protection of Freedoms Act 2012 when referring to use of biometric data.

- It follows guidance from the Department for Education (DfE) Generative artificial intelligence in education

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

3. Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, individual. This may include the individual's: ● Name (including initials) ● Identification number ● Location data ● Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special Categories of Personal Data	Personal data, which is more sensitive and so needs more protection, including information about an individual's: ● Racial or ethnic origin ● Political opinions ● Religious or philosophical beliefs ● Trade union membership ● Genetics ● Biometrics (such as fingerprints, retina and iris patterns), were used for identification purposes ● Health -physical or mental Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.

Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Our schools and central team process personal data relating to parents, pupils, staff, trustees, governors, visitors and others, and therefore is a data controller.

CET is registered as a data controller with the ICO and will renew this registration yearly or as otherwise legally required.

5. Roles and responsibilities

- **Trust Board**
  The Trust Board has overall responsibility for ensuring that schools within our Trust comply with all relevant data protection obligations.

- **Data Protection Officer**
  The data protection officer (DPO) is the person responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, developing related policies and guidelines where applicable.

  The DPO will provide an annual report of their activities directly to the CEO, who will report to the Board their advice and recommendations on data protection issues. Our DPO can be contacted via admin@cetrust.org.uk

- **Data Champions**
  The data champion is usually the office manager within each school, this person acts as the representative of the data controller on a day-to-day basis in each school. To be the first point of contact for GDPR questions (where applicable), to log data breaches, subject access requests, freedom of information requests and reports back to the DPO.

- **CEO/Headteachers**
  The CEO/Headteacher has overall responsibility for GDPR and data control within their school.

- **All staff**
  Staff are responsible for collecting, storing and processing any personal data in accordance with this policy. Informing their school or Trust of any changes to their personal data.

  In the first instance contact their data champion, with any concerns that this policy is not being followed or where a personal data breach may have taken place.

  Contact the DPO with the above. Also, questions about the operating of this policy, data protection law, retaining personal data or keeping personal data secure. Whenever they are engaging in a new activity that may affect the privacy rights of individuals.

  If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK.

  If they need help with any contracts or sharing personal data with third parties.

6. Data protection principle

The UK GDPR is based on data protection principles that our schools and Trust must comply with. The principles say that personal data must be:

- Personal data shall be processed fairly, lawfully and in a transparent manner.
- Collected for specific, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary to fulfil the purpose(s) for which it is being processed.
- Accurate and where necessary, kept up to date.
- Kept no longer than is necessary for the purpose for which it is processed.
- Processed in a way that ensures appropriate security.

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 the 6 ‘lawful basis’ (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school/Trust can **fulfil a contract** with the individual, or the individual has asked the school/Trust to take specific steps before entering a contract.
- The data needs to be processed so that the school/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 school/Trust, as a public authority, **can perform a task in the public interest**, or exercise its **official** authority.
- The data needs to be processed for the **legitimate interests** of the school/Trust or 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 their **consent**.

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.

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law.

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent.**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law.**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of consent.
- The data has already been made **manifestly public** by the individual.
- The data needs to be processed for the establishment, exercise or defence of **legal claims.**
- The data needs to be processed for reasons of **substantial public interest** as defined by legislation.
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obligated to confidentiality under law.
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obligated to confidentiality under law.
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purpose and the processing is in the public interest.

For criminal offence data, we meet both a lawful basis and a conditional set out under data protection law. Conditions include:

- The individual (or parent/carer when appropriate in the case of a pupil) has given **consent.**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made **manifestly public** by the individual.
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**.
- The data needs to be processed for the reasons of **substantial public interest** as defined in legislation.

When we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified explicit and legitimate reasons. We will explain their reasons to 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 Trusts records retention schedule.

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but not limited to:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils, for example - IT companies. We will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that comply with UK data protection law.
    - Establish a contract with the supplier or contractor 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 the service.

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

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 staff or pupils.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

9. Subject access requests and other rights of individuals

Individuals have the right to make a subject access request (SAR) to gain access to personal information that the Trust and schools holds about them.

Further information about the rights of access, including how to make a subject access request can be found in our Subjects Access Request policy.

10. Parent requests to see the educational record

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

This right applies as long as the pupil concerned is aged under 18.

11. CCTV

Any schools within the Trust that use closed circuit television (CCTV) images, to ensure the school site remains safe and secure environment for pupils, staff, visitors and other individuals.

For further information, please refer to our Trust's CCTV policy.

12. Biometric recognition systems

The Trust does not use biometric recognition systems.

13. Photographs and videos

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

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

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

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

See our individual school safeguarding policies for more information on photographs and videos. Please refer to the Trust Subject Access Request (SAR) policy.

14. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. The Trust recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots. If personal and/or sensitive data is entered into an unauthorised generative AI tool, the Trust will treat this as a data breach, and will follow the personal data breach procedure outlined in our Data Breach policy.

Please refer to our Trust AI policy.

15. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purposes of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6).
- Completing data protection impact assessments (DPIA) where the Trust and school's processing of personal data presents a high risk to rights of freedoms of individuals, and when introducing new technologies (the DPO will advise on this process).
- Integrating data protection into internal documents including this policy, any related policies and privacy notices

- Regularly training members of staff on data protection law, this policy, any other data protection matters, we will also keep a record of attendance.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Appropriate safeguards being put in place if we transfer any personal data outside the UK, where different data protection laws may apply.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact detail of our Trust DPO and all information we are required to share about how we use and process their personal data (via our privacy notices).
    - For all personal data we hold, maintaining an internal type of data, data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards of those, retention periods and how we are keeping the data secure.

16. 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.
- Paper containing confidential personal date must not be left on office and classroom desks, on staff-room tables, pinned to notice/display boards, or left anywhere else where there is general access (please refer to the Trust's clear desk and screen policy).
- Where personal information needs to be taken off site, staff must sign an acceptable use agreement, which is reviewed and re-signed annually.
- Passwords must be at least 8 characters long containing the 3 random word technique.
- Encryption software is used to protect all portable devices such as laptops.
- All removable media such as hard drives and USB devices are encrypted.
- Staff, pupils, trustees, or governors who store personal information on their personal devices are expected to follow the same security procedures as for school/Trust owned equipment (see online safety/acceptable use agreements).
- Where we need to share personal data with a third-party, we carry out diligence and take responsible steps to ensure it is stored securely and adequately protected (see section 8).

17. 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 or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with UK data protection law.

18. Personal data breaches

The Trust and schools will make reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, the incident should be reported to the school's data champion, where the incident will be logged. Once logged, incidents will be investigated, and appropriate remedial action undertaken. The DPO will be informed and consulted as required.

Where appropriate, we will report the data breach to the ICO within 72 hours. Please refer to our Data Breach Policy.

19. 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 school's processes make it necessary.

20. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed every 2 years and shared with the Trust board.

21. Links with other policies

This data protection policy is linked to our:

- Acceptable use agreements
- Clear desk and clear screen
- CCTV
- Data breach

- Freedom of information
- Online safety
- Privacy notices
- Safeguarding