Unique Policy Number: 23.2

Data Breach 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	**March 2024**	**KW**	*New policy*

Owner: DPO
Approver: Trust Board
Statutory Policy: Yes
Review Cycle: 2 years **Approval date**: 28th March 2024

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.

This policy aims to ensure that adequate controls are in place so that data breaches are identified, and action is taken quickly. Actions should be proportionate, consistent and transparent.

CET holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible.

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)
- Article 33 0f the UK General Data Protection Regulations
- Article 34 0f the UK General Data Protection Regulations

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 Category Data	Special category 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 or sex life or sexual orientation
Personal Data Breach	A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.
Data subject	The identified or identifiable living individual whose personal data is held or processed.
Date processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Third Party	Individuals who are not the subject of the data, but may be connected to or affected by it is known as a third party.
ICO	The Information Commissioner's Office, the UK's independent regulator for data protection and information.

4. Responsibilities

The Trust has an overall responsibility to put in place clear policies and procedures and to monitor these processed to ensure that measures have been implemented and remain appropriate and effective.

- **Trust Board**
  The Trust Board has overall responsibility for ensuring that schools within the 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 compliance with data protection law, developing related policies and guidelines where applicable, support and advise schools within the Trust.

- **Central Trust Team**
  On some occasions there maybe records held centrally, in these cases the Central Team will be responsible for providing the relevant schools Data Champion with the requested information.

Each school within the Trust will ensure that they have designated staff who are appropriately trained to ensure requests made are handled appropriately, in accordance with this policy and processes herein.

- **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-today basis in each school. To be the first point of contact for GDPR questions (where applicable), to log and respond to data breeches, subject access requests, freedom of information requests and reports back to the DPO.

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

- **All staff**
  Are responsible for notifying the Data Champion of within each School as quickly as possible.

5. What is a data breach?

According to the ICO, organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data.

A data breach is “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”.

A personal data breach may mean that someone outside the school gets unauthorised access to personal and/or special category (sensitive) data. But a personal data breach can also occur if there is unauthorised access within the school for example an employee accidentally or deliberately alters or deletes personal data.

5.1 A data security breach can happen for many reasons:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- ‘Blagging’ offences where information is obtained by deceiving the organisation who holds it

5.2 Human error

This the most common cause of data breaches. These can happen for many reasons:

- Theft or loss of paperwork
- Data posted to incorrect recipient
- Data sent by email to incorrect recipient
- Failure to redact personal/sensitive data.

5.3 What is a near miss?

A near miss is an event that does not result in a data breach, but which had the potential to do so. Examples of such events might include data that was misplaced but found quickly internally or data that was sent out but was identified and returned.

Our school is committed to identifying weaknesses in our operational procedures. Each school will record all near misses in order to understand patterns, learn lessons and implement improvements.

6. Notifying the ICO

The DPO or CEO will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.

This will be done without undue delay and, where possible, within 72 hours of becoming aware of the breach. The 72 hours deadline is applicable regardless of school holidays (I.e. it is not 72 working hours). If the School is unsure of whether to report a breach, the assumption will be to report it.

7. How can a data breach be managed?

When an incident occurs, there are four important elements to the incident management plan:

- Containment and recovery;
- Assessment of on-going risk;
- Notification; and
- Evaluation and response

The UK GDPR and DPA places a duty on all organisations in the UK to report certain types of data breach to the ICO. In some cases, organisations will also have to report certain types of data breach to the individuals affected.

7.1 Containment and recovery

Containment and recovery involves limiting the scope and impact of the data breach and stemming it as quickly as possible.

The person discovering a data breach should take the following steps immediately:

Report it to their school's Data Champion or, in their absence the Headteacher. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable. A reporting form must be completed.

The Data Champion/Headteacher, must quickly take appropriate steps to ascertain full details of the breach, determine whether the breach is still occurring, recover any losses and limit the damage. Steps might include:

- Attempting to recover any lost equipment or personal information
- Shutting down an IT system
- Contacting the Office team and other key departments so that they are prepared for any potentially inappropriate enquiries about the affected data subjects
- If an inappropriate enquiry is received, staff should attempt to obtain the enquirer's name/contact details and confirm that they will ring the enquirer back
- The risk owner organising, with the approval of the Senior Leadership Team, for a school-wide email to be sent
- The use of back-ups to restore lost, damaged or stolen information
- If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use
- If the data breach includes any entry codes or passwords then these codes must be changed immediately, and the relevant organisations and members of staff informed.
- The Headteacher/CEO be prepared to handle any press enquiries or to make any press releases

At any stage through this initial process the school will seek support and/or advise from the DPO when deemed necessary.

7.2 Assessment and investigation

If a data breach is identified, then a formal assessment and investigation should be commenced by the designated member of staff (data breach owner) who should determine the seriousness of the breach and the risks arising from it. Specifically, the data breach owner should identify

- Whose information was involved in the breach
- What went wrong
- The potential effect on the data subject(s)
- What immediate steps are required to remedy the situation
- What lessons have been learnt to avoid a repeat incident.

In order to support this process, the data breach owner should complete the Data Breach Report form.

7.3 The investigation should consider:

- The type of information
- Its sensitivity
- How many individuals are affected by the breach?
- What types of people have been affected (the students, parents, staff etc)?

- Whether those affected have any special needs/vulnerabilities
- What protections are in place (e.g. encryption)?
- What happened to the information?
- Whether the information could be put to any illegal or inappropriate use
- What could the information tell a third party about the individual?

Actions to contain and recover data as well as mitigate any risk should be taken immediately. The investigation is to ensure that the case is being managed and any improvement actions agreed are implemented. The investigation should be proportionate to the breach identified and risk of harm.

Some level of investigation might be required to carry out the Risk Assessment and determine the most appropriate route of escalation. If, once identified, risk of a data breach is contained and does not pose immediate further threat to the school and/or students, timeframes for official escalation/notification can be extended to allow for a more thorough investigation. Extensions must be agreed at each stage and noted in the report.

As an investigation proceeds, the risk may change, and the reporting requirements should be amended in line with the change in risk. For example, a case identified as a significant risk initially may increase to a major risk and therefore should be escalated to the ICO

Advice, input and support can be sought from the DPO as required.

7.4 Notification, evaluation and response

The ICO requires us to inform those affected where there is a significant breach of personal and sensitive data and the risk of harm to those individuals is high.

If there was a high risk of further harm the school would have an obligation to disclose the breach to each individual affected. However, this has to be balanced against the risk of causing further distress and anxiety to the families and individuals by informing them about the breach.

The ICO guidance states that “informing people about a breach is not an end in itself. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.”

When determining whether it is necessary to notify individuals directly of the breach, the Data Champion, Headteacher/CEO from the school will co-operate with and seek guidance from the DPO, the ICO and any other relevant authorities.

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the school will consider alternative means to make those affected aware (for example by making a statement on the school website.

The school will need to consider whether other parties need to be notified of the breach. For example:

- Insurers
- Parents
- Third parties (for example when they are also affected by the breach); Local authority
- The police

This list is non-exhaustive

The DPO should assess and evaluate whether any changes need to be made to the Trust's and schools processes and procedures to ensure that a similar breach does not occur.

Staff must not communicate directly with the press, treat all potential data breaches as confidential unless otherwise instructed by the CEO, Headteacher or DPO.

The Headteacher/CEO of the relevant school should be prepared to handle any press enquiries or to make any press releases if and when required.

8. Preventing future breaches

Once the data breach has been dealt with, the School/Trust with the advice from the DPO will consider its security processes with the aim of preventing further breaches. In order to do this, we will:

- Establish what security measures were in place when the breach occurred
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice
- Consider whether it's necessary to conduct a privacy or data protection impact assessment
- Consider whether further audits or data protection steps need to be taken

Reporting Data Protection Concerns

Prevention is always better than dealing with data protection as an afterthought. Data security concerns may arise at any time, and we would encourage you to report any concerns (even if they don't meet the criteria of a data breach) that you may have to your schools Data Champion, Head teacher or the DPO. This can help capture risks as they emerge, protect the Schools and Trust from data breaches and keep our processes up to date and effective.

9. Data breach log

All data breaches, including near misses, will be recorded on the data breach Log within each school by the Data Champion, also all logs to be reported to the DPO. All issues identified by the application of this policy will be recorded in the data breach log and categorised according to whether it is a data breach or near miss.

This information will be reviewed and analysed at least half termly to identify patterns and monitor the implementation of agreed service improvements.

The DPO will report the findings, trends and lessons learnt to the CEO, who will report to the Governors and Trustees.

10. Training

Where policy or procedure changes are introduced, all staff should be informed of the changes and required to record their acknowledgement of reading and understanding the changes via Access.

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.

11. Links with other policies

This CCTV policy is link to our:

- Data protection
- Privacy notices
- Subject access requests
- Freedom of information

Personal Data Breach Report Form

If you discover a personal data security breach, please notify the Data Champion (or Headteacher, in their absence) immediately.

Please complete this form and return to the Data Champion within your school as soon as possible.

Part 1 (for use by any staff)

Notification of Data Security Breach	
Date(s) of breach:	
Date incident was discovered:	
Name of person reporting incident:	
Name of school where the incident occurred:	
Brief description of incident or details of information lost:	
Categories and approximate number of people whose data has been breached:	
Categories and approximate number of data records concerned:	
Brief description of any actions taken since breach was discovered, including measures to mitigate the effects:	
Likely consequences of the data breach:	

Information passed onto:	**Time:**	**Date:**
Form completed by **Name (print):** **Signature:**	**Job title:**	

Part 2 (for use by DPO)

Report received by DPO:	**Date:**	**Time completed:**	**From whom:**	
Any advice sought, if applicable	**Date:**	**Time completed:**	**From: name/organisation:**	
	Advice received:			
Assessment made and action taken	**Date:**	**Time completed:**	**By whom:**	
Breach reported to ICO? **Yes/N/A**	**Date:**	**Time completed:**	**By whom:**	
Name of DPO				
Signature:			**Date:**	