

*At Weaver Trust, we work to ensure that all in our community believe, belong, and thrive. This policy is informed by our Trust's vision of inspiring all to believe in their own ability to achieve their full potential, both academically and socially. By living by our values of being innovative, responsible and caring, we create powerful learning communities - positively impacting all.*

## 1. Policy Statement

1.1 This notice explains what personal data (information) we hold about you, how we collect it, how we use it, and how we may share it. We are required to give you this information under data protection law.

## 2. Definitions

Term	Definition
Trust	Is Weaver Trust Limited, Suite 2, Oak Tree Barn, Hatton Lane, Warrington, WA4 4BX and its subsidiary organisations, and clubs, collectively referred to as the 'Trust'
Department for Education (DfE)	Is the government department which deals with education
Local Authority (LA)	is Cheshire West and Chester Council, The Portal, Wellington Road, Ellesmere Port, CH65 0BA or Halton Borough Council, Municipal Building, Kingsway, Widnes, Cheshire, WA8 7QF
Chief Executive Officer (CEO)	Is Annette Williams
Chair of Trustees	Is Julian Cobley
Data Protection Coordinator	Is Phil Atkinson
Trust Data Protection Officer (DPO)	Is Tru-Digital Protection T/A Tru-Digital Services Ltd, 5 Brayford Square, London, E1 0SG <a href="mailto:dpo@trudigital.co.uk">dpo@trudigital.co.uk</a>
Data Controller	Is the Trust for UK data protection law
<a href="#">Data Protection Act</a> (DPA)	The Data Protection Act 2018 makes a provision about the processing of personal data, which is subject to GDPR, with an amendment in 2023.
<a href="#">Freedom of Information Act</a> (FOI)	The Freedom of Information Act 2000 discloses information held by public authorities or persons

	providing services for them and amends the Data Protection Act.
<a href="#">UK General Data Protection Regulation (GDPR)</a>	which applies across the European Union (including in the United Kingdom)
<a href="#">Education Act (EA)</a>	The Education Act 1996 consolidates the Education Act 1944 and certain other educational enactments.
<a href="#">Information Commissioners Office (ICO)</a>	This organisation ensures compliance with the Data Protection Act, Freedom of Information Act, and GDPR and handles formal complaints.

### 3. Introduction

3.1 In line with the GDPR, the School has a responsibility to ensure that all records are only kept for as long as is necessary. This policy outlines the retention periods for the information and records that we process, applying to all information, regardless of format.

### 4. Roles and Responsibilities

4.1 Roles and responsibilities include:

- The School has a responsibility to maintain its records and record-keeping systems in accordance with the regulatory environment. The Data Protection Officer has overall responsibility for this policy.
- The Data Protection Coordinator in the school will provide guidance to staff on good records management practices and promote compliance with this policy.
- All employees must ensure that records for which they are responsible are accurate and maintained. At the end of their retention period, it is their responsibility to ensure that such records are disposed of in accordance with this policy.

### 5. How Long Should We Keep Our Records

5.1 Records should be kept for as long as they are needed to meet the operational needs of the Trust, together with legal and regulatory requirements. We have assessed our records to:

- Determine their value as a source of information about the Trust, its operations, relationships and environment.
- Assess their importance as evidence of business activities and decisions.
- Establish whether there are any legal or regulatory retention requirements (including: Public Records Act (1958), the FoI, the Limitation Act (1980), the DPA).

5.2 Where records are likely to have a historical value, or are worthy of permanent preservation, we may choose to archive them at the end of any retention period.

5.3 Where information is to be archived or destroyed, schools must carry out such processing by no later than the

start of the new Academic Year after the expiration of the retention period.

## 6. Retention Schedule

6.1 The retention schedule has been produced in line with the advice and guidance provided by the Information Record Management Society (IRMS).

6.2 This may not be a complete list, and where education settings are unsure about specific retention periods, they should consult the DPO for further guidance.

6.3 The schedule suggests several actions that can be taken to dispose of information once it has reached the end of its retention period:

- Regular disposal: Records can be placed in a normal rubbish bin or skip.
- Secure disposal: ‘must be shredded’- Information is likely to be so sensitive it must be shredded on site, by a member of staff, and not left waiting for collection by an external company. For information to be considered securely disposed of, it must be in a condition where it cannot be read or reconstructed. Skips and regular waste disposal will not be regarded as secure. Paper records must be shredded using a cross-cutting shredder, pulped or burned. CDs/ DVDs and other storage media should be destroyed into particles no larger than 6mm. Any electronic data should be deleted alongside any back-ups.
- Review: At the end of the retention period, a review may be necessary to ascertain whether a further retention period is required beyond the one advised. If a further retention period isn’t essential, the information must be securely disposed of.
- Transfer: At the end of the retention period, the information may be transferred to another establishment. In such cases, the information should be sent securely via encrypted email or other secure electronic means, by recorded delivery, or delivered by hand.

## 7. Child Protection Records

7.1 You’re no longer required to indefinitely retain records on child sexual abuse.

7.2 Previously, it was an offence to destroy any records relevant to the Independent Inquiry into Child Sexual Abuse (IICSA). This requirement overrode UK data protection laws—see section 21 of the Inquiries Act 2005.

7.3 The IICSA has now concluded, so this is no longer included as a requirement in Keeping Children Safe in Education 2023.

7.4 You should now treat records that contain information about allegations of sexual abuse in the same way as any other information about claims made against staff. For more guidance, please see the section below. Keeping records of allegations made against staff.

7.5 There is No Statutory Retention Period.

7.5.1 Apart from the above rules, there are no specific regulations on how long you should keep child protection records, but you:

- Must not keep more personal information on file than is absolutely necessary under the

UK General Data Protection Regulation (UK GDPR)

- Should refer to your local authority (LA) when setting your own retention schedule, as LAs may set retention periods for schools in their area

7.6 Records Stored in the Pupil File

- 7.6.1 If you keep child protection reports or disclosures in the pupil file, store them in a separate area of the record or in an individual, linked file.
- 7.6.2 Keep the records for the same length of time as the pupil file, which is:
  - Until the child has left the school, for primary schools
  - For 25 years from the child's date of birth, for the school where the child completes their compulsory education
- 7.6.3 When a pupil leaves primary school, send their file to their new school. Read this article for more advice on transferring child protection files securely.

7.7 Records Stored in Separate Files

- 7.7.1 If you keep child protection information in separate files, keep them for 25 years from the child's date of birth and then review whether you still need them.

7.8 Keeping Copies Once Pupils Have Transferred

- 7.8.1 There is no specific statutory guidance on how long records should be kept after a pupil transfers to another school—LAs have differing policies.
- 7.8.2 You should keep a copy of the file in case, for example, it's later lost by another person. However, you should check this with your LA or legal provider.

7.9 Keeping Records of Allegations Made Against Staff

- 7.9.1 If allegations of abuse made about a member of staff were found to be malicious or false, remove details of those allegations from personnel records.
- 7.9.2 For all other allegations:
  - Keep a clear and comprehensive summary of the allegation, including details of how it was followed up, how it was resolved, any action taken, any decisions reached, and the outcome.
  - Provide a copy of the report to the person concerned, where agreed by children's social care or the police.
  - Keep a declaration on whether the information will be referred to in any future reference.
  - This is to make sure:
  - Accurate information can be given in response to requests for a reference in future.
  - Clarification can be given where future DBS checks reveal information about allegations that did not result in a criminal conviction.
- 7.9.3 Records of allegations should be retained at least until the accused person has reached normal pension

age, or for a period of 10 years from the date of the allegation if that is longer.

7.9.4 This is set out in paragraphs 415 to 417 of the statutory safeguarding guidance, Keeping Children Safe in Education (KCSIE) 2023.

7.10 Keeping Court Orders Relating to Pupils

7.10.1 Under the requirements of UK data protection law, you must not keep more personal information on file than is necessary. Therefore, you should only keep a copy of a court order relating to a pupil if having this extra information would be helpful.

7.10.2 The DfE told us that if the order relates to a specific safeguarding issue, you may wish to see and retain a copy of the court order to ensure you have enough information to keep the pupil safe—but you should decide what is appropriate.

7.10.3 In most cases, the DfE and Information Commissioner's Office both said it would be better for you to record:

- There's a court order in place for the pupil.
- Who informed the school of the court order?
- What arrangements does the school need to have in place to support the court order?

7.10.4 Whether you keep a copy of the order or just records relating to it, you must:

- Make sure that this information is kept securely.
- Put arrangements in place to prevent unauthorised access.
- Abide by the other data protection principles when handling sensitive personal data of this nature.

**8. Using a Third Party**

8.1 Schools may choose to use an external company to support them with their secure disposal. If doing so, academies must carry out checks to ensure that the company is reputable and will destroy the documents securely.

8.2 There should be a contract and a data processing agreement in place with the company to ensure that they will comply with the DPA and GDPR.

8.3 A record of disposal should also be maintained (see record keeping).

**9. Monitoring**

9.1 The Data Protection Coordinator will review this policy annually, or more frequently if required, and liaise with the DPO.

**Approved by:**

**Chair of Trust**

**CEO**

**Date:**