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
Trust Finance and Operations Manager	Is Heather Cashin
Chair of Trustees	Is Julian Cobley
Trustees	Are Craig Ridge, Matt Lord, Rob Foreman, Chris Heptinstall, Eve Bartlet, Kathy Hardy, and Roxi Corp
Trust Governance and Communications Manager	Is Phil Atkinson
Trust Data Protection Officer (DPO)	Is Tru-Digital Protection T/A Tru-Digital Services Ltd, 5 Brayford Square, London, E1 0SG dpo@trudigital.co.uk

Data Protection Act (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.
Freedom of Information Act (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.
UK General Data Protection Regulation (GDPR)	which applies across the European Union (including in the United Kingdom)
Educations Act (EA)	The Education Act 1996 consolidates the Education Act 1944 and certain other educational enactments.
Information Commissioners Office (ICO)	This organisation ensures compliance with the Data Protection Act, Freedom of Information Act, and GDPR and handles formal complaints.
Personal Data	Any information relating to an identified or identifiable living 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), are used for identification purposes

	• Health – physical or mental • Sex life or sexual orientation
Data Subject	The identified or identifiable individual whose personal data is held or processed
Data Controller	Is the Trust for UK data protection law
Electronic Solution	Means the software or services, whether on-premise or cloud-based, that are essential for the Trist's operations
Criminal Convictions Data	Personal data relating to criminal convictions and offences, including Personal Data relating to criminal allegations and proceedings
Data Privacy Impact Assessment (DPIA)	Tools and assessments are used to identify and mitigate the risks associated with a data processing activity. A DPIA can be carried out as part of privacy by design and should be conducted for all primary system or business change programmes involving the processing of Personal Data

3. Introduction

3.1 Under UK data protection law, individuals have a right to be informed about how our Trust uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes referred to as 'fair processing notices') to individuals when we are processing their data.

3.2 This privacy notice explains how we collect, store, and use personal data about pupils, parents and individuals who are interested in working at our Trust.

3.3 This policy must be approved by the Trustees and signed by the Chief Executive and the Chair of Trustees.

4. Why do we Process Special Categories of Personal Data and Criminal Convictions Data

4.1 We process Special Categories of Personal Data and Criminal Convictions Data for the following purposes, where this is under our data protection policy:

- To carry out our legal obligations under employment law;
- For preventative or occupational medicine to assess an employee's working capacity and/or the need for reasonable adjustments; • complying with health and safety obligations;
- Complying with the Equality Act 2010 and in the interests of ensuring equal opportunities and treatment.
- Checking applicants' and employees' right to work in the UK;
- Verifying that candidates are suitable for employment or continued employment;

- To carry out our legal and statutory obligations concerning Trust governance;
- Verifying that governors and trustees are ideal for the role;
- To administer and pay trade union premiums and register the status of a protected employee.
- To safeguard our pupils and other individuals.
- To support individuals with a particular disability or medical condition;
- To protect the data subject's vital interests where they are not able to provide their consent;
- To prevent or detect crime without the consent of the data subject, so as not to prejudice those purposes where it is necessary for reasons of substantial public interest.

5. Personal Data Protection Principles

5.1 The GDPR mandates that personal data be processed in accordance with the six principles outlined in Article 5(1). Article 5(2) requires controllers to demonstrate compliance with Article 5(1).

5.2 We comply with the principles relating to the Processing of Personal Data set out in the GDPR, which require Personal Data to be:

- Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);
- Collected only for specified, explicit and legitimate purposes (Purpose Limitation);
- Adequate, relevant, and limited to what is necessary for the purposes for which it is processed (Data Minimisation);
- Accurate and kept up to date where necessary (Accuracy)
- Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is processed (Storage Limitation); and
- Processed in a manner that ensures security through appropriate technical and organisational measures to prevent unauthorised or unlawful processing, as well as accidental loss, destruction, or damage (Security, Integrity and Confidentiality).
- We are responsible for and must be able to demonstrate compliance with the data protection principles outlined above (Accountability).

6. Compliance with Data Protection Principles

6.1 Lawfulness, Fairness, and Transparency

6.1.1 Personal data must be processed lawfully, fairly, and transparently with regard to the Data Subject. We shall process Personal Data solely in a manner that is fair and lawful, and for purposes that are specifically designated.

6.1.2 Furthermore, the processing of Special Categories of Personal Data and Criminal Convictions Data shall only occur where there exists a lawful basis for such processing, and where one of the specified conditions related to these categories applies. For each processing activity, we will identify and

document the relevant legal basis and the specific processing condition utilised.

6.1.3 In instances where we collect Special Categories of Personal Data and Criminal Convictions Data directly from Data Subjects or indirectly from third parties or publicly accessible sources, we will provide Data Subjects with a comprehensive privacy notice. This notice outlines all information mandated by the GDPR, presented concisely, transparently, intelligibly, and in plain, accessible language that can be easily understood.

Type of Special Categories of Personal Data/Criminal Convictions Data Processed	Lawful Basis for Processing	Conditions for Processing Special Categories of Personal Data/Criminal Convictions Data
Data concerning health	Compliance with a legal obligation (Article 6 (1) (c)) or necessary for the performance of a contract with the Data Subject (Article 6 (1) (b))	Necessary for performing or exercising obligations or rights which are imposed or conferred by law on the controller or the Data Subject in connection with employment, social security or social protection. (Paragraph 1(1)(a), Schedule 1, DPA 2018.) Necessary for health and social care purposes. (Paragraph 2(1), Schedule 1, DPA 2018.) To provide support for individuals with a particular disability or medical condition. (Paragraph 16(1), Schedule 1, DPA 2018.) Necessary for the provision of confidential counselling, advice or support or of another similar service provided confidentially. (Paragraph 17(1), Schedule 1, DPA 2018.)
Racial or ethnic origin data	Compliance with a legal obligation (Article 6 (1) (c))	Necessary for performing or exercising obligations or rights which are imposed or conferred by law on the controller or the Data Subject in connection with

		employment, social security or social protection. (Paragraph 1(1)(a), Schedule 1, DPA 2018.)
Criminal Convictions Data	Compliance with a legal obligation (Article 6 (1) (c)) OR In the organisation's legitimate interests (Article 6 (1) (f)) which are not outweighed by the fundamental rights and freedoms of the Data Subject	Necessary for performing or exercising obligations or rights which are imposed or conferred by law on the Controller or the Data Subject in connection with employment, social security or social protection. (Paragraph 1(1)(a), Schedule 1, DPA 2018.) Meets one of the substantial public interest conditions set out in Part 2 of Schedule 1 to the DPA 2018 (such as: Preventing or detecting unlawful acts (Paragraph 10(1), Schedule 1, DPA 2018). Protecting the public against dishonesty, etc. (Paragraph 11(1), Schedule 1, DPA 2018.) Complying with, or assisting other persons to comply with, a regulatory requirement which involves a person taking steps to establish whether another persona has committed an unlawful act; or been involved in dishonesty, malpractice or other seriously improper conduct (Paragraph 12(1), Schedule 1, DPA 2018). Preventing a specific type of fraud. (Paragraph 14(1), Schedule 1, DPA 2018.) Necessary for:

		Protecting an individual from neglect or physical, mental or emotional harm, or Protecting the physical, psychological or emotional well-being of an individual Where the individual is under the age of 18, or is 18 or over and at risk. (Paragraph 18(1), Schedule 1, DPA 2018.)
Equal Opportunity Data	In the organisations's legitimate interests (Article 6 (1) (f)) which are not outweighed by the fundamental rights and freedoms of the Data Subject	Necessary for identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people specified concerning that category to enable such equality to be promoted or maintained. (Paragraph 8(1)(b), Schedule 1, DPA 2018.)

7. Purpose Limitation

7.1 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

7.2 We will only collect Personal Data for specified purposes and will inform Data Subjects of these purposes in a published privacy notice. If we plan to use personal data for a new purpose (other than a legal obligation or function set out in law), we will check that this is compatible with our original purpose. We will not use Personal Data for new, different, or incompatible purposes from those disclosed when it was first obtained, unless we have informed the Data Subject of the new purposes and they have given their consent where necessary.

8. Data Minimisation

8.1 Personal Data shall be adequate, relevant and limited to what is necessary concerning the purposes for which it is processed.

8.2 We will only collect or disclose the minimum Personal Data required for the purpose for which the data is collected or disclosed. We will ensure that we do not collect excessive data and that the Personal Data collected is adequate and relevant for the intended purposes. We will periodically review the Personal Data and delete any information that is no longer needed.

9. Accuracy

9.1 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when it is inaccurate.

9.2 We will ensure that the Personal Data we hold and use is accurate, complete, kept up to date, and relevant to the purpose for which it is collected by us. We verify the accuracy of any Personal Data at the point of collection and at regular intervals subsequently. We undertake all reasonable measures to destroy or amend inaccurate or outdated Personal Data.

9.3 Each school periodically dispatches staff and pupil data to facilitate data subjects in verifying the accuracy of the information and sends regular reminders to staff and parents regarding the significance of informing Trust of any changes to their data.

9.4 As outlined in our Trusts' data protection policies, Data Subjects possess the right to request rectification. The Trust's data protection policies outline how the Trust consider and complies with any requests related to this right of rectification.

9.5 Our Data Protection Policies can be found on our websites.

10. Storage Limitation

10.1 We retain Personal Data solely for the duration necessary to fulfil the purposes for which it was originally collected, or to comply with any legal obligations. Once the data is no longer required, it shall be either deleted or anonymised permanently.

10.2 We ensure that Personal Data is deleted once it is no longer necessary for the purposes it was collected, unless a legal requirement mandates its retention for a longer period.

10.3 Data Subjects will be informed of the duration for which their data is stored and the criteria used to determine this period in any applicable privacy notices.

11. Security, Integrity, Confidentiality

11.1 Personal Data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures. We will analyse any risks presented by our processing to assess the level of security required.

11.2 Security procedures include

- Entry Controls: Any stranger seen in entry-controlled areas should be challenged and reported to a staff member.
- Secure lockable desks and cupboards: Desks and cupboards containing confidential information should be kept locked and secured. (Personal information is always regarded as confidential.)
- Methods of disposal: Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the Information Commissioner's Office guidance on the disposal of IT assets

(see DPO for details).

- Equipment: Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.
- Reports shall be stored electronically using the Trust's Electronic Solution.
- Medical Plans will be exhibited within the first aid rooms, the canteen, and other designated areas throughout the Trust as deemed necessary. Care must be exercised to ensure that the information remains inaccessible to passers-by.
- Working away from the Trust premises – paper documents:
    - We acknowledge the necessity for staff to remove documents from the premises to fulfil their statutory responsibilities, such as marking, reporting, and data analysis.
    - Documents containing minimal personal data, such as pupils' workbooks, are considered to be of low risk and may be appropriately taken home by staff members. This practice is also practical, as it facilitates easier marking of student work by teachers.
    - Documents containing substantial personal information, such as pupil records, assessment data, and reports, that are removed from the site must be stored in a closed folder and kept in a secure location.
    - Pupil information collected during an off-site educational visit must be returned to the trip leader, who will then refile or dispose of it appropriately.
    - Staff should avoid leaving documents in their car as this creates a higher risk of them being stolen.
    - When returning documents to the Trust, staff should take them immediately to their original storage place.
- Working away from the Trust premises – electronic working:
    - Electronic documents containing substantial personal data must be stored on an encrypted pen drive or within a secure cloud-based environment. The use of personal laptop hard drives to store this type of data is NOT permitted.
- Document printing: Documents containing personal data must be collected immediately from printers and not left on photocopiers.
- Scanned documents: Documents must be deleted from the scanned folder immediately after they have been saved securely.

12. Accountability Principle

12.1 We are responsible for and able to demonstrate compliance with these principles. Our DPO is responsible for ensuring that we are compliant with these principles. Any questions about this policy should be submitted to the DPO.

12.2 We will:

- Ensure that records are kept of all Personal Data processing activities, and that these are

provided to the ICO on request.

- Conduct a DPIA for any Personal Data processing that is likely to result in a high risk to Data Subjects' interests, to understand how Processing may affect them, and consult the ICO if appropriate.
- Ensure that a DPO is appointed to provide independent advice and monitoring of Personal Data handling, and that the DPO has access to report to the highest management level.
- Have internal processes in place to ensure that Personal Data is only collected, used, or handled in a manner that is compliant with these principles.

13. Review

12.1 No condition for processing and associated information will be removed from this policy until the expiry of 6 months following the end of the period during which the Trust undertakes that processing activity.

12.2 The policy will be retained where we process Special Categories of Personal Data and Criminal Convictions Data, and any earlier versions will be retained for a minimum of six months after we cease such processing.

12.3 A copy of this policy will be provided to the ICO on request and free of charge. For further information about our compliance with data protection law, please contact our DPO.

Approved by: _____ _____

Chair of Trust **CEO**

Date: _____ _____