HOLLINGWORTH LEARNING TRUST
STAFF WORKFORCE PRIVACY POLICY

Reviewed:	Spring 2026
Version:	7.1
Next Review:	**Live Document:** To be updated as and when new advice and guidance is received regarding Data (Use and Access) Act 2025, UK GDPR and Freedom of Information.
Approved By:	**To be reviewed by Trustees every 12 months**

VERSION INFORMATION

Version	Reason for Update	Author	Date	Approved By:
1	Original Policy	S Collinge S Pearson J Hawkrigg	Summer 2018	CEO
2	Update in line with further guidance re Data Protection, GDPR and FOI	S Collinge	Spring 2020	CEO
3	Review and Update	S Collinge	Spring 2021	CEO
4	Review and Update	S Collinge	Spring 2022	CEO
5	Review and Update	S Collinge	Spring 2023	Trustees
6	Review & Updated Updates to sections 2,3 & 4 to include filtering and monitoring, in line with KCSIE 2023	S Collinge	Spring 2024	Trustees
7	Review and Update Update to section 3	S Collinge	Spring 2025	Trustees
7.1	Review and Update	S Collinge	Spring 2026	Trustees

Contents

1. Introduction 4
2. The personal data we hold 4
3. Why we collect and use this data 5
4. Our lawful basis for using this data 5
5. Collecting this data 6
6. How we store this data 7
7. Who we share data with 7
8. Your rights 8
9. Complaints 8
10. Contact us 9

1. Introduction

Under UK data protection law, individuals have a right to be informed about how Hollingworth Learning Trust ("the Trust") uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about **individuals we employ, or otherwise engage to work at our trust**.

Hollingworth Learning Trust is the 'data controller' for the purposes of data protection law.

Our Data Protection Officer is Ms Susan Collinge (see 'Contact us' below).

2. The personal data we hold

Personal data that we may collect, use, store, and share (when appropriate) about you includes, but is not restricted to:

- Personal information, including contact details, date of birth, marital status, and gender.
- Contact information, including next of kin and emergency contact numbers.
- Contract information, including salary, annual leave, pension, and benefits information.
- Finance information, including bank account details, payroll records, national insurance number and tax status information.
- Recruitment information, including copies of right to work documentation, references and other information included in an application form or letter or as part of the application process.
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships.
- Safeguarding and pre-employment checks information, including copies of ID, certificates, and necessary pre-employment checks.
- Performance information.
- Outcomes of any disciplinary and/or grievance procedures.
- Absence data.
- Biometric Information.
- Access Information, including car information and movements around the building.
- Information about your use of our information and communication systems, equipment, and facilities (e.g. school computers).

We may also collect, use, store, and share (when appropriate) information about you that falls into "special categories" of more sensitive personal data. This includes, but is not restricted to, information about:

1. Disclosed medical information, including any health conditions you have that we need to be aware of.
2. Sickness records.
3. Digital imagery and CCTV images captured in our schools.
4. Trade union membership.

Please note, this list is not exhaustive, to access the current list of categories of information we process please contact the Data Protection Officer.

We may also collect, use, store and share (when appropriate) information about criminal convictions and offences.

We may also hold data about you that we have received from other organisations, including other schools, local authorities and social services, and the Disclosure and Barring Service in respect of criminal offence data.

3. Why we collect and use this data

We use the data listed above to:

a) Enable you to be paid.
b) Facilitate safe recruitment, as part of our safeguarding obligations towards pupils.
c) Support effective performance management.
d) Inform our recruitment and retention policies.
e) Allow better financial modelling and planning.
f) Enable equalities monitoring.
g) Improve the management of workforce data across the sector.
h) Support the work of the School Teachers' Review Body.
i) Meet statutory duties placed upon us for DfE data collections.
j) Collect digital imagery and biometric information for systems in our schools.
k) Keep staff safe (medical conditions, emergency contacts details).
l) Make sure our information and communication systems, equipment and facilities (e.g. school computers) are used appropriately, legally and safely.

We will only use your personal information for the purposes for which we have collected it, unless we reasonably consider that we need to use it for another purpose. If we need to use your personal information for an unrelated purpose, we will notify you and explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent in compliance with the above rules where this is required or permitted by law.

3.1 Use of your personal data in automated decision making and profiling.

We do not currently process any personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

3.2 Use of your personal data for filtering and monitoring purposes

While you're in any of our trust's schools, we may monitor your use of our information and communication systems, equipment and facilities (e.g. school computers). We do this so that we can:

- Comply with health and safety and other legal obligations.
- Comply with our policies (e.g. child protection policy, IT acceptable use policy) and our legal obligations.
- Keep our network(s) and devices safe from unauthorised access, and prevent malicious software from harming our network(s).

4. Our lawful basis for using this data

Under the General Data Protection Regulation (GDPR), our lawful bases for processing your personal data for the purposes listed in section 3 above are as follows:

For the purposes of **(a), (c), (d), (e)** and **(f)**, in accordance with the **'public task'** basis, collecting and processing data is necessary to perform tasks that schools are required to perform as part of their statutory function.

For the purposes of **(b), (g), (h), (i)** and **(l),** in accordance with the **'legal obligation'** basis, the Trust is required to collect and process data to meet our responsibilities under law as set out here:

- Safer Recruitment and Safeguarding obligations
- Data collected for the DfE Census
- Section 537A of Education Act 1996
- The Education Act 1996 s29(3)
- The Education (School Performance Information) (England) Regulations 2007

- Regulations 5 and 8 School Information (England)Regulations 2008
- The Education (Pupil Regulations) (England)(Amendment) Regulations 2013

For the purposes of **(j),** in accordance with the **'consent'** basis, staff will be asked for consent by the Trust to process this information.

For the purposes of **(k)**, in accordance with the **'vital interests'** basis, the Trust will process this data to keep staff safe.

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent and explain how you will go about withdrawing consent if you wish to do so.

4.1 Our basis for using special category data.

For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and one of the following conditions for processing as set out in data protection law:

- We have obtained your explicit consent to use your personal data in a certain way.
- We need to perform or exercise an obligation or right in relation to employment, social security, or social protection law.
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent.
- The data concerned has already been made manifestly public by you.
- We need to process it for the establishment, exercise, or defence of legal claims.
- We need to process it for reasons of substantial public interest as defined in legislation.
- We need to process it 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 obliged to confidentiality under law.
- We need to process it for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law.
- We need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest.

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing, as set out in data protection law. Conditions include:

- We have obtained your consent to use it in a specific way.
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent.
- The data concerned has already been made manifestly public by you.
- We need to process it for, or in connection with, legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights.
- We need to process it for reasons of substantial public interest as defined in legislation.

5. Collecting this data

While the majority of information we collect about you is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Most of the data we hold about you will come from you, via application forms, pre-employment checks and data checking forms, but we may also hold data about you from:

- Local authorities and previous employers/schools.
- Government departments or agencies.
- Police forces, courts, tribunals.

6. How we store this data

We hold personal information about you securely while you are employed at our trust. We will also store your information securely beyond your employment at our trust for the set amount of time as shown in our data retention schedule. For more information on our data retention schedule and how we keep your data safe, please visit http://irms.org.uk/page/SchoolsToolkit

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your personal data securely when we no longer have a legal requirement to retain it.

7. Who we share data with

We do not share information about you with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law), we may share personal information about you with:

- **Rochdale Borough Council**
  We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

- **Government Departments and Agencies, including the Department for Education**
  The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our children and young people with the Department for Education (DfE) for the purpose of those data collections, under: Section 537A of the Education Act 1996.
  We are required to share information about our trust employees with the (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.
  All data is transferred securely and held by the DfE under a combination of software and hardware controls which meet the current government security policy framework.

- **Ofsted**

- **Our suppliers and service providers**
  As part of the academy's day to day procedures, it will share information about pupils to approved systems on the Trust's data ecosystem. To view the full list of Trust's systems please visit the Trust website www.hltrust.co.uk

- **Financial organisations**
- **Our auditors**
- **Survey and research organisations**
- **Health authorities**
- **Security organisations**
- **Health and social welfare organisations**
- **Professional advisers and consultants**
- **Charities and voluntary organisations**
- **Police forces, courts, tribunals**

7.1 Transferring data internationally

We may share personal information about you with the following international third parties outside of the European Economic Area, where different data protection legislation applies:

- Other schools or educational establishments
- Government departments or agencies
- Storage of school data on app or cloud server providers

Where your personal data is transferred to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

In cases where we have to set up safeguarding arrangements to complete this transfer, you can get a copy of these arrangements by contacting us.

8. Your rights

8.1 Requesting access to the personal data we hold about you.

Under data protection legislation, you have the right to request access to information we hold about you. You have a right to make a 'subject access request' to gain access to personal information that we hold about you.

If you make a subject access request, and if we do hold information about you, we will (subject to any exemptions that may apply):

- Give you a description of it.
- Tell you why we are holding and processing it, and how long we will keep it for.
- Explain where we got it from, if not from you.
- Tell you who it has been, or will be, shared with.
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this.
- Give you a copy of the information in an intelligible form.
- If you make a Subject Access Request (SAR), we may ask you for clarification to help us locate the data you need. Under the Data (Use and Access) Act 2025, the statutory time limit for our response may be paused ('stopped the clock') until we receive this clarification from you.

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact us (see 'Contact us' below).

8.2 Your other rights regarding your data.

Under data protection law, you have certain rights regarding how your personal data is used and kept safe. For example, you have the right to:

- Object to our use of your personal data.
- Prevent your data being used to send direct marketing.
- Object to and challenge the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person).
  (We do not currently use automated decision-making processes that produce legal or similarly significant effects. If this changes, we will update this notice and implement suitable safeguards including the right to human intervention.)
- In certain circumstances, have inaccurate personal data corrected.
- In certain circumstances, have the personal data we hold about you deleted or destroyed, or restrict its processing.
- In certain circumstances, be notified of a data breach.
- Make a complaint to the Information Commissioner's Office.
- Claim compensation for damages caused by a breach of the data protection regulations.

To exercise any of these rights, please contact us (see 'Contact us' below).

9. Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/make-a-complaint/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Please note that under the Data (Use and Access) Act 2025, the ICO may typically expect you to have raised your concern with us and given us an opportunity to respond before they will investigate a complaint.

10. Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **Data Protection Officer**:

- Ms Susan Collinge, Compliance Manager on 01706 292828 or via email at dpo@hltrust.co.uk
- In writing to the Trust at: Hollingworth Learning Trust
Suite 1, Floor 1
Hafley Court
Buckley Road
Rochdale
OL12 9DJ
- Our Local Authority: http://www.rochdale.gov.uk/