Workforce Privacy Notice

Followed by Three Towers AP Academy

Adopted: Spring Term 2026

Reviewed: Annually (or as required when statutory guidance is updated)

Reviewer: Trust Data Protection Officer (DPO)

1 Introduction

The Rowan Learning Trust collects, holds, uses and shares information about our workforce. Much of the information we collect is classed as 'personal data' and our use of it is covered by a set of rules called the General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 and the Data Protection Act 2018 as amended by the Data (use and Access) Act 2025 (DUAA 2025).

For the purposes of Data Protection legislation the Rowan Learning Trust is a data controller and is registered as such with the Information Commissioner's Office.

You have rights around the data collected, including knowing how and why we are processing the data. "Processing" data means everything from collecting, to storing, using, sharing and disposing of it.

The Trust workforce includes all those employed to teach, or otherwise engaged to work, either on a paid, contracted or voluntary basis, for the Central Team or at any of our schools/academies.

This document tells you more about:

- The information we collect;
- What we use the information for;
- How your information is stored and how long we keep it;
- What rights you have to the information.

2 What Information do we collect and use about staff?

Under the DUAA, organisations must demonstrate that the purposes for which data is collected are proportionate and clearly justified. The Trust documents these purposes as part of its accountability obligations.

We collect many different categories of information, for example:

- Personal details – such as name, address, employee or teacher number, national insurance (NI) number;
- Next of kin and emergency contacts.
- Recruitment information – including job application details, selection & interview records, references received, right to work documentation;
- Qualifications (and where relevant, subjects taught)
- Identity verification records;
- Checks made regarding your online presence including social media searches;
- Contract information – such as start date, hours worked, post, roles and salary information;
- Banking information – such as bank details, account numbers, account holders;
- Taxation details;
- Pension details;
- Records of transactions;
- Car insurance and MOT details;

- Performance assessment details including information for improving performance;
- Information relating to grievance and/or disciplinary procedures, as outlined in those respective policies;
- Work absence information – such as annual leave records; leave of absence records; medical appointments;
- Records of communications – such as emails you have sent and received;
- Photographs of you or images on CCTV*;
- Information about your use of Trust/school IT devices and networks;
- Information about consultation with other professionals;

We also are required to collect and use information that is given additional protection under the GDPR – **special category data**, including:

- Characteristics information - such as gender, age, ethnicity;
- Information about medical or health conditions, including whether you have a disability for which we need to make reasonable adjustments;
- Sickness-related absences;
- Demographic information required for monitoring equal opportunities – such as ethnicity, sexual orientation, health and religion or belief;
- Information about criminal convictions, offences and prohibitions where this is necessary for compliance with our other legal and regulatory obligations. This information may have come from other organisations including former employers, Teacher Regulation Agency, social care and the Disclosure & Barring Service.
- Details of trade union membership if you pay your subscriptions through payroll.

However, this will only be undertaken where and to the extent it is necessary for a lawful purpose in connection with your employment or other engagement to work for the Trust/school.

Whilst the majority of information we collect is mandatory, there is some information that can be provided voluntarily. Whenever we seek to collect information from you, we make it clear whether providing it is mandatory or optional.

In addition:

- Schools also use CCTV cameras around their site(s) for security purposes and for the protection of staff, learners and visitors. CCTV footage may be referred to during the course of disciplinary procedures (for staff or learners) or to investigate other issues.
- The school may record external telephone calls for training and monitoring purposes. Personal data referred to within such a call recording may be transcribed and/or referred to when supporting student learning, when supporting students' health/welfare (including their vital interests) or when resolving other issues.

3 Why we collect and use this information.

We use the information to:

- Meet our statutory duties, including our legal obligations to share information;

- Facilitate safer recruitment (e.g. by carrying out criminal records checks and requesting references);
- Safeguard children;
- For health and safety including site security and safety;
- Enable photographic images to be used for identification purposes (safeguarding), and celebration purposes (to record work, classes and school events)
- Enable individuals to be paid;
- Support the management of absence;
- Support you in your job role and help you to deliver the best support of our learners and your colleagues;
- Support effective performance management e.g. identifying professional development needs and providing appropriate training;
- Enable you to pay for meals in school;
- Enable the development of a comprehensive picture of the workforce and how it is deployed;
- Allow better financial modelling and planning;
- Protect public monies against fraud;
- Detect crime and prevent crime and combat potential fraud;
- Streamline systems;
- Keep you up to date with news about the school.

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 any other reason and that reason is incompatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and explain the legal basis that allows us to do so.

4 The legal basis for using this information

Depending on the purpose, our use of your information will be legal due to one of the following:

- Informed consent given by you [Article 6(1)(a)]
  For example: The use of banking information in our payment service
- To meet the terms of a contract [Article 6(1)(b)
  For example: Your contract of employment
- To meet a legal requirement [Article 6(1)(c)]
  For example: Section 5 of the Education (supply of Information about the School Workforce)(England) Regulations 2007 and amendments
- To protect the vital interests of you or someone else [Article 6(1)(d)
  For example: Giving your family details to emergency services
- Delivering a public task [Article 6(1)(e)]
  For example: Keeping records of meetings with parents
- For legitimate interests [Article 6(1)(f)

Recognised Legitimate Interests [Article 6(1)(ga)] (Updated for DUAA 2025)

In some circumstances, we process personal data under the Data (Use and Access) Act 2025 using a recognised legitimate interest. This applies where processing is necessary for certain pre-approved public-interest purposes (for example, safeguarding, preventing or detecting crime, or regulatory compliance). Where this applies, we ensure the processing is proportionate and transparent.

The ways we collect and use special category workforce information are lawful based on:

- Explicit consent
- For compliance with certain legal obligations
- For exercising certain legal rights
- For protecting a person's vital interests in an emergency
- For health and public health reasons
- For carrying out tasks that are in the substantial public interest including for safeguarding purposes.

Where we use special category data, we process this under the following exemptions from Section 9 of GDPR:

- Explicit consent is given by you [Article 9(2)(a)]
  For example: Use of biometric information to identify you for the catering system;
- Information used in the field of employment [Article 9(2)(b)]
  For example: Using information about your ethnic origin or any disability for equality monitoring purposes
- To protect the vital interest of you or someone else [Article 9(2)(c)]
  For example: Providing details of any medical/health conditions you have in the event of an emergency
- For substantial public service [Article 9(2)(g)]
  For example: Using information about your health to ensure a safe working environment

Biometric Systems – where a school operates a biometric system for staff identification (where used, these are usually fingerprint-based systems found in catering and library applications but can include door entry and other systems) then the school will require explicit written consent from each intended user.

Marketing purposes - Where a family member gives us consent, we may send them marketing information by text message or email, such as promoting school events, campaigns or charities. **Consent can be withdrawn at any time by contacting us (see the Contacts section)**

Automated decision making & profiling - We do **not** use any personal information to make automated decisions about our learners or their families, or to profile them. If automated or algorithmic decision-making systems are introduced in the future which could significantly affect learners or families, we will update this notice to explain the decision-making logic and your right to request **human review**, in line with DUAA requirements.

Filtering and Monitoring Purposes – We monitor the use of our ICT network and equipment. We do this so that we can:

- Comply with Health & Safety and other legal obligations;
- Comply with our policies, including Safeguarding & Child Protection, Online Safety, Remote Learning and Acceptable Use of ICT as well as other statutory obligations;
- Keep our networks and devices safe from unauthorised access and prevent malicious software from harming our networks.

5 Collecting this information

We collect this information in a variety of ways, including but not limited to:

- your application form;
- your passport or other identity documents such as your driving license;
- forms completed by you at the start of or during employment (such as pension benefit nomination forms, medical forms completed at the start of your employment);
- correspondence with you;
- interviews, meetings or other assessments with you;
- self-certification forms and/or fit Notes;
- images provided by individuals or taken using school photographic equipment;
- our CCTV systems;
- the Department for Education (teacher registration and Section 128);
- the DBS Service and Teaching Regulation Agency;
- the police;
- the NHS;
- the local authority;
- previous employers e.g. through references prior to employment;
- social media checks (in line with KCSIE guidance).

We sometimes audio/video record sessions/lessons/assessments for learners or staff development and assessment. This will generate personal data including staff images, names, contributions, and will be protected, processed and retained in the same way as all personal data, in line with the Trust's Data Protection Policies. Recordings in these circumstances will also be carried out in line with our HR policies.

Workforce data is essential for the Trust's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it is requested on a voluntary basis. We will inform you at the point of collection, whether you are required to provide certain information to us and your rights in relation to this.

6 Storing your personal data

The DUAA requires public-sector organisations to maintain clear accountability records, including documented processing activities, data-sharing decisions, and evidence of staff data-protection training. The Trust maintains these measures as part of its compliance obligations.

Anyone visiting one of our sites is required to sign in using Inventry. Data collected during this process, including digital images is stored on a standalone hard drive which is encrypted.

Details of Inventry's Privacy Notice can be found here InVentry Privacy Notice - Education | InVentry

Some of the personal data that we collect and use/process is stored in the Trust's Microsoft 365 account. This is a cloud-based platform with personal data being held on Microsoft servers based within the EU. Other data, depending on why we use it will be kept on other systems (see Section 8) or in paper files which are held in secure storage. We also use email to enable authorised users to transfer information to one another. These emails are always encrypted.

Most of the personal data that we collect and use is added to your personnel file. Other data, depending on its purpose, will be kept in other systems or in manual files. We use email to enable authorised users to transfer information to one another.

Some personal data is kept for different lengths of time. For example.

- your personnel file is for 6 years after the date you leave employment;
- annual appraisals are kept for the current year and then for 5 years;
- records of any accident you have at work are kept for 12 years after the incident.

We dispose of all personal information securely when we no longer need it.

If you would like to know how long we keep a specific piece of personal data, please contact the Data Protection Lead whose details can be found at the end of this Privacy Notice.

Governance and accountability (Updated for DUAA 2025) *– The DUAA increases expectations on public bodies to evidence strong governance, including appropriate staff training, transparent data-sharing decisions, and documented records of processing. We maintain appropriate governance measures to meet these requirements.*

7 Requesting access to your personal data and other rights

Right of Access - you have the right to access/view the personal data that we hold about you, to receive a copy of the data and to be given more information about the data including any transfer to countries who do not fall under the requirements of the GDPR. Some information we hold cannot be accessed in this way. If you ask for information that is not available, there may be other ways of accessing it and we can help you.

To have access to your personal data we will need to collect details of what you want and in the first instance you can contact the Data Protection Lead whose details can be found at the end of this Privacy Notice.

Subject Access Requests: DUAA 2025 changes (Updated for DUAA 2025)

When responding to a Subject Access Request (SAR/DSAR):

- *we will conduct only reasonable and proportionate searches as required by the Data (Use and Access) Act 2025; and*
- *we may **pause the statutory response timeframe** where we need additional information to verify your identity or to clarify the scope of your request; you will be notified if this happens*

You also have the right to:

- **be informed** about the collection and use of your personal data;
- **correction** - have inaccurate personal data corrected/rectified, or completed if it is incomplete;
- **be forgotten** - have your data erased, often known as the 'right to be forgotten'; however this does not apply where, amongst other things, processing is necessary to comply with a legal obligation;
- **restriction** - limit the way we are using your information, although, as above this is a limited right;
- **objection** - object to the way we are using your information; though other than for marketing purposes, this is also limited as above.

Other Rights you have

You also have rights in relation to automated decision making and profiling, though these are not currently relevant as we do not carry out automated decision making or profiling.

Right to withdraw consent - where we rely on your consent to collect and use personal data, you have the right to withdraw that consent. This applies if you change your mind, or you are unhappy with our use of your personal data. **Withdrawing your consent will need to be recorded in writing, please contact the Data Protection Lead at school.** Once we receive this, we will stop using your data.

Right to complain - Data Protection Complaints Process (mandatory under DUAA 2025) (Updated for DUAA 2025)

Before raising a concern with the ICO, the DUAA 2025 requires that you first use the Trust's internal data-protection complaints procedure. To make a complaint:

- contact the Data Protection Lead in the first instance;
- if unresolved, the matter will be considered under the Trust's internal data-protection complaints procedure;
- you may then escalate to the ICO once the internal process is complete.

We may refuse your information rights request for legitimate reasons, which depend on why we are processing it. Some rights may not apply in these circumstances:

- Your right to have all personal data deleted or destroyed does not apply when the lawful basis for processing is legal obligation or public task;
- Your right to receive a copy of your personal data, or have your personal data transmitted to another controller, does not apply when the lawful basis for processing is legal obligation, vital interests, public task or legitimate interests;
- Right to object to the use of your private data does not apply when the lawful basis for processing is contract, legal obligation or vital interests. And if the lawful basis is consent, you do not have the right to object, but you have the right to withdraw consent.

8 Sharing your personal data

At times we will share your personal data with other organisations and people. We will only do this when we are legally required to do so, when our policies allow us to do so or when you

have given your consent. In some instances, we may be required to include special category data in the information we provide.

Examples of people we share personal data with are:

- Local Authority (LA) (to meet our legal obligations to share certain information with it, such as safeguarding concerns);
- Our Local Governing Committee (LGC) and/or Trust Board;
- The Department for Education, including the Teaching Regulation Authority;
- The Disclosure and Barring Service (DBS);
- HMRC;
- Employers/training providers where references are required;
- Family, associates and representatives of the person whose personal data we are processing who are authorised to receive the data;
- Police and/or Courts;
- Other authorities/agencies for safeguarding purposes;
- Healthcare, social and welfare organisations;
- Voluntary and charitable organisations;
- Our suppliers and service providers used by school (and our Trust) to carry out day-to-day processes and requirements. For example, but not limited to:
    - Arbor – our MIS system;
    - UHY – our payroll provider;
    - Microsoft 365 and TEAMS – our workspace including emails;
    - Fohcus – our occupational health provider;
    - Online SCR – used to manage our single central record;
    - School photographer;
    - Social media platforms such as X, Instagram and Facebook.
    - Schools to add their biometrics company for catering if appropriate.

Where we share your personal data with someone who is a supplier or service provider, we have taken steps to ensure that they treat your personal data in a way that meets the requirements of the GDPR.

8.1 International Transfers

Where personal information is transferred outside the UK or EEA, we apply the DUAA "data protection test", ensuring that the level of protection in the destination country is **not materially lower** than that in the UK. Appropriate safeguards (including International Data Transfer Agreements) are used where required. Personal information may be transferred outside the UK and the European Economic Area ('EEA'), including to the United States.

Where information is transferred outside the UK or EEA to a country that is not designated as "adequate" in relation to data protection law, the information is adequately protected by the use of International Data Transfer Agreements and security measures, and other appropriate safeguards. For more information on international transfers please contact us to speak to our

Data Protection Officer.

8.2 Freedom of Information Act and environmental Information Regulations 2004

As a public body, both TTAPA and our Trust are subject to requests made under the above legislation. Therefore, we have a legal obligation to process any personal data we hold when considering requests under these laws. For example, we may receive a request asking about numbers of staff with particular levels of professional qualification.

However, we will never disclose personal data in our responses to these requests where to do so would contravene the principles of data protection.

9 Why we regularly share school workforce information

We do not share information about our workforce members with anyone without consent unless the law and our policies allow us to do so.

10 How Government use your information

We share personal data with the Department for Education (DfE) on a statutory basis. We are required to share information about our employees with DfE under 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 Security policy framework - GOV.UK.

For more information about the Department's data sharing process, please visit: How DfE shares personal data - GOV.UK

The workforce data we share with the DfE through data collections:

- Informs departmental policy on pay and the monitoring of the effectiveness and diversity of the Trust workforce;
- Links to our funding and expenditure;
- Supports 'longer term' research and monitoring of educational policy.

There is a link on our website to the DfE's

10.1. Data collection requirements

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision).

All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to: Data collection and censuses for schools - GOV.UK

10.2 Sharing by the Department

The DfE may share information about school employees with third parties who promote the

education or well-being of children or the effective deployment of school staff in England by:

- Conducting research or analysis;
- Producing statistics;
- Providing information, advice or guidance.

The Department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use.

Decisions on whether the DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- Who is requesting the data;
- The purpose for which it is required;
- The level and sensitivity of data requested; and
- The arrangements in place to securely store and handle the data.

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

If you need more information about how the DfE collects and uses your information, please visit: How DfE shares personal data - GOV.UK

10.3 How to find out what personal information the DfE hold about you

Under the terms of the Data Protection Act 2018, you are entitled to ask the Department:

- if they are processing your personal data;
- for a description of the data they hold about you;
- the reasons they're holding it and any recipient it may be disclosed to;
- for a copy of your personal data and any details of its source.

If you want to see the personal data held about you by the Department, you should make a 'subject access request'. Further information on how to do this can be found within the Department's personal information charter that is published at the address below: Personal information charter - Department for Education - GOV.UK (www.gov.uk)

To contact the DfE please visit: Contact the Department for Education (DfE) - GOV.UK (www.gov.uk)

11 Updates to this privacy notice

We may need to update this privacy notice periodically, so we recommend that you revisit this information from time to time. ***Further ICO guidance on DUAA changes is expected during 2026 and we will reflect this in updates (Updated for DUAA 2025).***

This version was approved in **November 2024 and updated in January 2026.**

12 Who to contact

The school and Trust have the responsibility to ensure that your personal data is protected: they are called the data controller. All members of staff work for the data controller. If you have a concern about the way we are collecting or using your personal data, or you have any

questions about this privacy notice, we request that you raise your concern with the school in the first instance.

We recommend that you contact the data protection lead (DPL):

Name of Person:	C Seggie
Email address:	hindleyoffice@ttapa.net
Contact number:	01942 932760 (select Hindley options)
Address:	Three Towers, Leyland Park House, Park Road, Hindley, WN2 3RX

If you are not satisfied with their response, please contact the Trust's Data Protection Administrator:

Name of Person:	Chris Bolton
Email address:	dpo@rlt.education
Contact number:	01942 939022
Address:	18 Beecham Court, Wigan, WN3 6PR

Trusts are also required to have someone called a Data Protection Officer or DPO. The DPO advises the Trust about issues to do with data protection, but can also help you, if you have a problem.

Our Data Protection Officer is:

Name of DPO:	GDPR Sentry Limited
Email address:	support@gdprsentry.com
Contact number:	0113 804 2035
Address:	Unit 434 Birch Park, Thorp Arch Estate, Wetherby, West Yorkshire, LS23 7FG

If you are dissatisfied with our response to your concerns, you can contact the ICO (contact details below) quoting our ICO registration number **ZA201403** and stating that the Data Controller is The Rowan Learning Trust.

Name:	Information Commissioner's Office
Contact number:	0303 123 1113 (local rate) or 01625 545745 if you prefer to use a national rate number
Address:	Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF
Website:	https://ico.org.uk/concerns/