

Ruth Miskin Literacy Limited Workforce and Recruitment Privacy Notice

This privacy notice has been written to inform prospective, current, and former employees about how and why we process their personal data, including during the recruitment process.

Who we are

Ruth Miskin Literacy Limited is a data controller as defined by the UK GDPR. This means that we determine the purposes for which your personal data is processed and how it is processed. We will only collect and use your personal data in a manner that is compliant with data protection legislation.

We have appointed our Head of Operations and Tech as our Data Protection Officer (DPO). The role of the DPO is to monitor our compliance with the UK GDPR and the Data Protection Act 2018 and advise on data protection issues. If you would like to discuss this privacy notice or our use of your data, please contact the DPO at support@ruthmiskin.com.

Personal information we collect

During a recruitment exercise, we will collect the following:

- Personal identifiers, including your name, contact details, date of birth, employee number, and national insurance number.
- Information about your right to work in the UK, including ID documents.
- Education and qualifications, including copies of certificates.
- Professional memberships and your qualified teacher status, where relevant.
- Your employment history, including employment references.
- Initial records of relevant criminal history data, including your DBS check.
- Information about your current salary level, including benefits and pension entitlements
- Information publicly available through online searches on shortlisted job candidates to identify any incidents or issues related to suitability to work with children that may need to be raised or clarified at the interview.
- Whether you have a disability which we need to make reasonable adjustments during the recruitment process
- Equality monitoring information, such as your ethnicity, religious beliefs and gender.

As well as retaining and updating some of the above information, during the course of your employment, we will also collect the following:

- Information about your workplace attendance and reasons for any absences.
- Information about professional development and performance, including reviews and any disciplinary information.

- Any updates to records of your criminal history, including your DBS check.
- Details of any internal or external continued professional development or training you completed.
- Emergency contact information.
- Financial and payroll data, including bank account information, tax, national insurance and pension contributions.
- Information contained in your contract, including your job role and responsibilities, start date, employment location, and contracted hours, etc.
- Medical information relevant to your employment, including any disability you disclose.
- Healthcare and medical information such as doctor details, allergies, medication and dietary requirements, vaccination details, etc.
- Photographs and/or video images of you, including CCTV footage which is recorded at the organisation's London Head Office (7 Sandy's Row).
- Records of communications and interactions we have with you.
- E-monitoring and filtering information about your use of our network and IT systems.

Why we collect your personal information

We process your information for the purposes outlined below:

- To ensure your right to work and assess your suitability for the role.
- To meet our safeguarding and health and safety obligations.
- To pay your salary and conduct related payroll functions.
- To monitor and manage staff absence.
- To monitor and manage professional development, training and performance.
- To make any reasonable adjustments you may need in relation to a health condition or disability.
- To promote the company, including in newsletters, on the company website, and social media platforms.
- To monitor and inform our policies on equality and diversity.
- When requested by you, to provide references to other organisations.

Our lawful basis for processing your information

Under the UK GDPR, it is essential to have a lawful basis when processing personal information. For workforce data processing, we normally rely on the following lawful bases:

- Article 6(1)(b) - contractual obligation
- Article 6(1)(c) - legal obligation

There may be occasions where our processing is not covered by one of the legal bases above. In that case, we may rely on Article 6(1)(f) - legitimate interests. We only rely on legitimate interests when we are using your data in ways you would reasonably expect.

If we share your information in a health emergency, we may rely on the lawful basis of Article 6(1)(d) – vital interests.

For the processing of personal data relating to criminal convictions and offences, processing meets Schedule 1, Part 2 of the Data Protection Act 2018 as below:

- Condition 10 - preventing or detecting unlawful acts
- Condition 18 - safeguarding of children and individuals at risk

Some of the information we collect about you is classed as special category data under the UK GDPR. The additional conditions that allow for processing this data are:

- Article 9(2)(b) - employment and social security, and social protection law
- Article 9(2)(g) - reasons of substantial public interest

The applicable condition in Schedule 1 of the Data Protection Act 2018 for Article 9(2)(b) is:

- Condition 1 - Employment, social security and social protection

The applicable substantial public interest conditions in Schedule 1 of the Data Protection Act 2018 are:

- Condition 6 - statutory and government purposes
- Condition 8 - equality of opportunity or treatment
- Condition 10 - preventing or detecting unlawful acts
- Condition 16 - support for individuals with a particular disability or medical condition
- Condition 18 - safeguarding of children and individuals at risk

If we share your information in a health emergency, we may rely on the additional condition of Article 9(2)(c) – vital interests.

Who we obtain your information from

We typically receive this information directly from you, for example, through documents and other records and information you provide during the job application or employment process. However, we may also receive some information from the following third parties:

- Official bodies, such as the Home Office and Disclosure and Barring Service.
- Your previous employers.
- Your nominated referees.

Who we share your information with

We may share your information with the following organisations:

- Disclosure and Barring Service (DBS).
- HM Revenue and Customs (HMRC).
- Department for Work and Pensions (DWP).
- Your pension provider.
- Private health care providers.
- Staff benefits provider, in relation to any salary sacrifice agreements.
- Our suppliers and advisors, including insurers, lawyers, consultants, and an accountant or payroll provider.
- Our IT application providers.
- Prospective future employers, landlords, letting agents, or mortgage brokers, where you have asked them to contact us for a reference.
- Emergency services, where required in a health emergency, including a mental health emergency.
- Customers, when sharing details of a trainer who will be providing our service.
- External travel agencies, where you consent to sharing, and we are arranging a booking on your behalf.

We may also share information with other third parties where there is a lawful basis to do so. For example, we may share information with the police for the purpose of crime detection or prevention.

How long we keep your information

We will retain your information in accordance with our Records Management Policy and Retention Schedule.

Much of the information will be retained for the duration of your employment plus 6 years. The retention period for most of the information we process about you is determined by statutory obligations. Any personal information which we are not required by law to retain will only be kept for as long as is necessary to fulfil its purpose.

International transfers of data

Although we are based in the UK, some of the digital information we hold may be stored on computer servers located outside the UK. Some of the IT applications we use may also transfer data outside the UK.

Usually, your information will not be transferred outside the European Economic Area, which is deemed to have adequate data protection standards by the UK government. If your information is transferred outside the EEA, we will ensure adequate safeguards are implemented as per UK GDPR.

What rights do you have over your data?

Under the UK GDPR, you have the following rights concerning the processing of your data:

- to be informed about how we process your personal data. This notice fulfils this obligation.
- to request a copy of the personal data we hold about you.
- to request that your personal data be amended if it is inaccurate or incomplete.
- to request that your personal data be erased where there is no compelling reason for its continued processing.
- to request that the processing of your personal data be restricted.
- to object to your personal data being processed.

If you have any concerns about the way we have handled your personal data or would like any further information, then please contact our DPO using the details provided above.

If we cannot resolve your concerns, you may also complain to the Information Commissioner's Office (ICO), the UK's data protection regulator. Its contact details are below:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113

ICO website: <https://ico.org.uk/make-a-complaint/data-protection-complaints/>

Changes to this notice

We reserve the right to change this privacy notice at any time. We will typically notify you of changes that affect you. However, please check regularly to ensure you have the latest version.

This privacy notice was last reviewed 10/09/2026.