Employee Privacy Notice

Applies to	Current and former employees, workers, volunteers, apprentices and consultants
Data controller	Anstey Horne & Co Ltd
Data Protection Lead	Stephen Walsh, COO - contact stevewalsh@ansteyhorne.co.uk
Version	1.0
Last reviewed	20/07/2026
Next review	20/07/2027

Important

This notice tells you how we collect, use and store personal data about you in connection with your employment or engagement with us. Please read it carefully. If you have any questions, contact the Data Protection Lead using the details above, or contact the HR Manager.

We are committed to processing your personal data securely, lawfully and transparently. This notice sets out what personal data we hold about you, why we hold it, how we use it, how long we keep it, who we share it with, and what your rights are.

We comply with our obligations under the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR) and the Data (Use and Access) Act 2025.

As your employer, we are the data controller in respect of your personal data. This means we determine the purposes and the means by which your personal data is processed.

1. The data we hold about you

We collect and process the following types of personal data about you:

Personal details

- Name, address, date of birth, email address and telephone numbers
- Photograph
- Gender and marital status
- Dependants, next of kin and their contact details
- Emergency contact details

Employment and contract information

- Current and previous job titles, job descriptions and pay grades
- Working hours and other terms and conditions of employment
- Start and end dates of employment
- Salary, pension entitlement and benefits
- Leave records including annual leave, family leave and sickness absence
- Training records and development plans

Recruitment information

- CV, application form, cover letter and interview notes
- References from previous employers
- Educational history and professional qualifications
- Membership of professional bodies
- Details of any pre-employment assessments

Identity and compliance

- Identification documents including passport and driving licence
- Immigration status and right to work documentation
- National Insurance number, tax code and bank details

Performance and conduct
- Performance information including appraisals and assessments against targets
- Letters of concern, formal warnings and documentation relating to disciplinary proceedings
- Documentation relating to grievance procedures

Electronic and other records
- Electronic information relating to your use of our IT systems
- Images captured by CCTV, photography or video

Special categories of personal data
Certain types of data are treated as particularly sensitive under data protection law and require additional protections. We may also hold and process the following special categories of data about you:

- Health and medical information, including information about any disability
- Racial or ethnic origin
- Sexual orientation
- Religion or belief
- Trade union membership
- Genetic or biometric data
- Political opinions

We hold and use special category data only where the law permits us to do so. We explain the specific purposes for which we use this data in section 3 below.

2. How we collect your data

We collect personal data from a variety of sources, usually beginning at the recruitment stage:

- directly from you - through your CV, application form, interview, forms completed at the start of employment, and ongoing interactions during your employment
- from third parties - including employment agencies, former employers (references), occupational health providers and credit reference agencies
- created internally - by your line manager or colleagues in the course of managing your employment, for example performance notes or absence records

Personal data is held in your personnel file and within our HR and IT systems.

3. Why we process your data

Data protection law requires us to have a lawful basis for processing your personal data. We rely on the following:

Performance of your contract
Most of the personal data we hold is necessary to carry out the employment contract between us. This includes paying you, managing your leave, administering your benefits and carrying out your contractual obligations.

Legal obligation
We are required by law to collect and process certain data. Examples include:
- confirming your right to work in the UK
- deducting and paying income tax and National Insurance to HMRC
- making reasonable adjustments for disability
- complying with health and safety legislation

Legitimate interests
We also process data where it is necessary for our legitimate business interests, provided those interests are not overridden by your rights. This includes:

- recruiting and making decisions about employment, promotion and remuneration
- managing your performance and conduct
- managing sickness absence

- maintaining accurate and up-to-date personnel records
- assessing training needs
- managing statutory leave and pay
- protecting the security of our IT and business systems
- preventing and detecting fraud
- business planning and restructuring
- defending legal claims brought against us

Special category data

We process special category data only where the law specifically permits. We most commonly do so:

- to carry out rights and obligations under employment law - for example, managing sickness absence, making reasonable adjustments for disability and monitoring equal opportunities
- where you have given explicit consent - we will always explain the reason and you can withdraw consent at any time without consequence
- where it is necessary to protect your vital interests or those of another person
- where you have already made the information public
- where processing is necessary for the establishment, exercise or defence of legal claims

In particular, we use special category data for equal opportunities monitoring, sickness absence management, and determining reasonable adjustments. We do not need your consent to process this data for those purposes.

4. Criminal conviction data

We will only collect and process data relating to criminal convictions or allegations where the nature of your role makes this appropriate and where the law permits. Where relevant, this data is collected at the recruitment stage and may also be collected during employment.

If we process criminal conviction data in relation to your role, we will inform you of the specific legal basis on which we do so and the purpose for which it is used.

5. If you do not provide your data

Some of the personal data we ask for is necessary to carry out our contractual and legal obligations. If you choose not to provide it, we may be unable to fulfil parts of our contract with you - for example, we cannot pay you without your bank details - or we may be prevented from complying with our legal obligations, such as confirming your right to work in the UK.

Where providing data is optional, we will make this clear.

6. Sharing your data

We share your personal data within the business only where necessary - for example, with your line manager for day-to-day management, and with those responsible for HR and payroll administration.

We share data with third parties only where required to do so, including:

- payroll providers and pension administrators
- occupational health providers
- former employers, when providing or verifying references
- HMRC and other regulatory bodies
- insurers where your data is relevant to a policy that relates to you

We may also share data with third parties in connection with a business sale, restructure or transfer, or where we are required to do so by law or a court order.

We require all third parties to whom we disclose your data to keep it confidential and secure, to process it only for the specified purpose and in accordance with our instructions, and to implement appropriate technical and organisational measures to protect it.

We do not transfer your personal data outside the United Kingdom. If that changes, we will inform you and explain what protections are in place.

7. How long we keep your data

We keep your personal data for as long as is necessary for the purposes for which it was collected. This will be at least for the duration of your employment or engagement with us. After your employment ends, we will retain certain data for a period of time in accordance with our data retention schedule - the length of time depending on the type of data and any legal requirements that apply.

You can ask the Data Protection Lead for details of the retention periods that apply to your data.

8. Automated decision-making

We do not make any decisions about you based solely on automated processing. All decisions that have a significant impact on you - such as those relating to your employment, performance or remuneration - involve human review and judgement.

9. Your rights

You have the following rights in relation to the personal data we hold about you. To exercise any of them, contact the Data Protection Lead.

The right to be informed
You have the right to know what data we hold about you and how we use it. This notice fulfils that obligation.

The right of access (subject access request)
You have the right to request a copy of the personal data we hold about you. This is called a subject access request (SAR) and must be made to the Data Protection Lead. We will respond within one month. There is no fee, though we may charge for requests that are manifestly unfounded or excessive.

The right to rectification
If any data we hold about you is inaccurate or incomplete, you have the right to ask us to correct it.

The right to erasure
In certain circumstances you can ask us to delete your personal data - for example, where we are no longer entitled to process it or where it is no longer necessary for the purpose for which it was collected.

The right to restrict processing
You can ask us to limit how we use your data while a correction or erasure request is being considered, or while you are contesting the lawfulness of our processing.

The right to object
You have the right to object to processing where we rely on legitimate interests as our lawful basis, if you believe your rights and interests outweigh ours. You also have the right to object to your data being used for direct marketing.

The right to data portability
You have the right to receive a copy of your personal data in a structured, commonly used and machine-readable format, and in some circumstances to have it transferred to another organisation.

The right not to be subject to automated decision-making
As set out above, we do not make solely automated decisions about you that have significant effects. You have the right to challenge any such decision if this changes.

The right to withdraw consent

Where we rely on your consent to process particular data, you have the right to withdraw that consent at any time. Withdrawing consent will not affect the lawfulness of processing carried out before withdrawal. There will be no adverse consequences for withdrawing your consent, though in some cases we may be able to continue processing on a different lawful basis.

10. Making a complaint

If you believe we have breached your data protection rights in any way, you can raise a complaint with us in the first instance by contacting the Data Protection Lead.

You also have the right to complain directly to the Information Commissioner's Office (ICO) at any time. The ICO is the supervisory authority for data protection in the UK. Full contact details and further information about your rights are available at www.ico.org.uk.

11. Contact details

Our Data Protection Lead is Stephen Walsh, Chief Operating Officer. They can be contacted at stevewalsh@ansteyhorne.co.uk.

If that person changes, you can find out who the current Data Protection Lead is by contacting the HR Manager or a Senior Director.

This notice will be updated from time to time. We will inform you of any significant changes.

This notice is issued under the Data Protection Act 2018, the UK General Data Protection Regulation and the Data (Use and Access) Act 2025.

Related document: Data Protection Policy