Data Protection Policy

Applies to	All current and former employees, workers, volunteers, apprentices and consultants
Data Protection Lead	Stephen Walsh, COO - contact stevewalsh@ansteyhorne.co.uk with any questions about this policy
Policy owner	HR Manager
Version	2.0
Last reviewed	20/07/2026
Next review	20/07/2027

Important

Our Data Protection Lead at the time of issuing this policy is Stephen Walsh. Any questions about this policy should be directed to them. If they are no longer the Data Protection Lead, contact the HR Manager or a Senior Director for current details.

We need to gather and use information about you as part of running our business and managing our relationship with you. This policy sets out how we handle that information, what your rights are as a data subject, and what your obligations are when handling personal data on our behalf.

We take data security and privacy seriously. We are committed to complying with the Data Protection Act 2018 (the '2018 Act'), the UK General Data Protection Regulation ('UK GDPR'), and the Data (Use and Access) Act 2025.

You should read this policy alongside your contract and any privacy notice we issue to you. This policy does not form part of your contract. We reserve the right to update it at any time. Where any conflict arises between this policy and the law, we will comply with the law.

1. Data protection principles

All personal data we hold must be processed in accordance with the following principles. It must:

- be processed fairly, lawfully and transparently
- be collected and processed only for specified, explicit and legitimate purposes
- be adequate, relevant and limited to what is necessary for those purposes
- be accurate and kept up to date - inaccurate data must be corrected or deleted without delay
- not be kept for longer than is necessary
- be processed securely

We are responsible for ensuring and demonstrating compliance with these principles.

2. What is personal data?

Personal data means any information that relates to a living person who can be identified from it, either on its own or together with other information we are likely to hold. It includes opinions about a person and indications of anyone's intentions in respect of them. It does not include anonymised data.

This policy applies to personal data in any form - electronic, paper or other materials.

Personal data may be provided by you, by someone else (such as a former employer, a doctor or a credit reference agency), or created by us - before, during or after your engagement with us.

Types of personal data we collect

We collect and use the following types of personal data:

- Recruitment information: application, CV, references, qualifications, professional memberships and pre-employment assessments
- Contact details and date of birth
- Emergency contact details
- Gender, marital status and family details
- Employment information: start and end dates, role and location, working hours, promotions, salary, pension, benefits and holiday entitlement
- Bank details and tax information including National Insurance number
- Identification documents including passport, driving licence, immigration status and right to work
- Information relating to disciplinary or grievance investigations or proceedings
- Performance and conduct information
- Training records
- Electronic information relating to your use of IT systems and telephone systems
- Images captured by CCTV, photography or video
- Any other category of personal data we notify you of from time to time

3. Special categories of personal data

Certain types of personal data are treated as more sensitive under data protection law and require additional protections. These 'special categories' include information about:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic or biometric data
- health
- sex life and sexual orientation

We may hold and use special category data where the law permits us to do so. We may also hold information about criminal convictions or allegations where this is relevant and lawful.

4. What is processing?

Processing means any operation performed on personal data, including collection, recording, organisation, storage, adaptation, retrieval, use, disclosure, combination, restriction, erasure or destruction. This includes both automated processing and manual processing of data held in a filing system.

5. How and why we process your personal data

We will process your personal data (including special categories where applicable) in line with the 2018 Act and the UK GDPR. We rely on the following lawful bases:

- performance of the contract between us
- compliance with a legal obligation
- our legitimate interests, where these are not overridden by your rights and interests

We can process your personal data on these bases without your knowledge or consent. We will not use your data for an unrelated purpose without first telling you and identifying the lawful basis we are relying on.

If you choose not to provide certain personal data, we may be unable to carry out parts of our contract with you - for example, we cannot pay you without your bank details, and we cannot make reasonable disability adjustments without relevant health information.

Examples of when we process your personal data

We process personal data at all stages of the employment relationship, including:

- deciding whether to employ or engage you
- determining your pay and contract terms
- checking your right to work
- carrying out and ending the contract
- training you and reviewing your performance
- managing absence, performance or conduct
- carrying out disciplinary or grievance investigations
- making reasonable adjustments for disability
- monitoring diversity and equal opportunities
- protecting the security of our business, systems, employees and customers
- monitoring and protecting health and safety
- paying salary, pension and other benefits
- paying tax and National Insurance
- providing references to prospective employers
- preventing and detecting fraud
- running and planning the business
- complying with legal and regulatory obligations
- defending the business in litigation or investigations

Processing special categories of personal data

We will only process special categories of your personal data where the law permits. We may do so without your consent where:

- it is necessary for carrying out employment law rights and obligations
- it is necessary to protect your vital interests or those of another person
- you have made the data public
- processing is necessary for the establishment, exercise or defence of legal claims
- processing is necessary for occupational health or assessment of your working capacity

Where we do need your consent, we will explain why and you are free not to give it. You can withdraw consent at any time by contacting the Data Protection Lead.

In particular, we use special category data as follows: race, ethnic origin, religion, sexual orientation and gender to monitor equal opportunities; health and sickness information to manage absence, assess fitness for work, pay benefits and comply with our legal obligations; and trade union membership to process subscriptions and comply with legal obligations.

6. Automated decision-making

We do not make decisions about you using automated processing alone, and we do not use profiling in our employment-related decisions. All decisions that affect you are made by people.

7. Smart devices and recording

Smart wearable devices - including smart watches, smart glasses and body-worn cameras - are capable of collecting personal data, including special category data, whether intentionally or inadvertently.

You must not use any smart wearable device or other personal device to record, photograph, film or capture data relating to colleagues, clients or third parties during working time, unless you have been explicitly authorised to do so.

Unauthorised recording using any device may constitute a data protection breach and will be treated as a serious disciplinary matter.

8. Sharing your personal data

We may share your personal data with contractors and agents who carry out functions on our behalf - for example, payroll providers. We require them to keep your data confidential and secure, to protect it in line with the law and our policies, and to use it only for the purpose for which it was shared and in accordance with our instructions.

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

9. Your obligations when handling personal data

Everyone who works for or with us has a responsibility to handle personal data properly. Much of the personal data we handle relates to our clients and their matters, and the same standards in this policy apply to it. In particular, you must:

- only access personal data you need for your work and are authorised to access
- only use data for the specified lawful purpose for which it was obtained
- not share personal data informally or with unauthorised people
- keep personal data secure - use strong passwords, lock your screen when away from your desk, lock drawers and filing cabinets
- not save personal data to personal computers or devices
- not take personal data off company premises without authorisation from your line manager or the Data Protection Lead
- not make unnecessary copies of personal data
- keep and dispose of copies securely - shred paper documents rather than binning them
- keep data accurate and up to date, including notifying us of changes to your own contact details
- consider whether data can be anonymised or pseudonymised to reduce risk
- not transfer personal data outside the United Kingdom without the authorisation of the Data Protection Lead
- ask the Data Protection Lead if you are unsure about any aspect of data protection

Any deliberate or negligent breach of this policy may result in disciplinary action under our Disciplinary Policy.

Concealing or destroying personal data that is subject to a subject access request is a criminal offence and would also constitute gross misconduct, potentially resulting in dismissal.

10. Data breaches

A data breach occurs when personal data is lost, disclosed to or accessed by an unauthorised person, or otherwise processed unlawfully. If you become aware of a potential data breach - whether involving your own data or anyone else's - you must contact the Data Protection Lead immediately and preserve any evidence you have.

We will assess the breach and, where it is likely to create a risk to individuals' rights and freedoms, notify the Information Commissioner's Office within 72 hours. Where the breach is likely to create a high risk to your rights and freedoms, we will also notify you directly.

11. Subject access requests

You have the right to ask us what personal data we hold about you. This is called a subject access request (SAR). SARs can be made verbally or in writing We encourage you to contact the Data Protection Lead so that we can identify and respond to your request promptly, but you do not have to use a particular form or wording.

We must respond within one month. If your request is complex or you have made multiple requests, we may extend this by up to two further months and will tell you if we are doing so.

There is no fee for an SAR. However, if a request is manifestly unfounded or excessive, we may charge a reasonable administrative fee or decline to respond

If you receive an SAR from anyone, forward it to the Data Protection Lead immediately. Do not attempt to respond yourself.

12. Your rights as a data subject

You have the following rights in relation to your personal data:

- The right to be informed about how and why we process your data - this policy sets that out
- The right of access - to request a copy of your personal data by way of an SAR
- The right to rectification - to have inaccurate data corrected by contacting the Data Protection Lead
- The right to erasure - to request that we delete your data where we are not legally entitled to process it or no longer need it
- The right to restrict processing - to ask us to limit how we use your data while a correction or erasure request is being considered
- The right to object - to challenge processing based on legitimate interests, or to object to direct marketing
- The right to data portability - to receive a copy of your data in a portable format, or to transfer it to another controller
- The right not to be subject to solely automated decision-making that has significant effects on you
- The right to be notified of a data breach that is likely to create a high risk to your rights and freedoms
- The right to withdraw consent - where consent is the basis for processing, you can withdraw it at any time

To exercise any of these rights, contact the Data Protection Lead. You also have the right to complain to the Information Commissioner's Office at any time - full details are at www.ico.org.uk.

13. Data retention

We will only retain personal data for as long as is necessary for the purposes for which it was collected. After that point it will be deleted or archived securely. We maintain retention schedules to ensure data is not kept beyond appropriate timeframes, and we will tell you in any applicable privacy notice how long your data is kept and how that period is determined.

14. Data protection complaints

If you believe we may have breached data protection rules in relation to your personal data, you can raise a complaint by contacting the Data Protection Lead in writing.

We will acknowledge your complaint within 30 days, investigate it thoroughly, keep you informed of progress and provide a written outcome.

You also have the right at any time to raise a complaint directly with the Information Commissioner's Office at www.ico.org.uk.

15. Questions and administration

The HR Manager is responsible for administering this policy. The Data Protection Lead is Stephen Walsh contactable at stevewalsh@ansteyhorne.co.uk. If that person changes, please contact the HR Manager or a Senior Director for current details.

Useful guidance on data protection is available at www.ico.org.uk.

Related policies: Employee Privacy Notice - Disciplinary Policy - Whistleblowing Policy

This policy does not form part of any contract of employment.