Privacy Notice for Employees, Workers and Contractors (GB)

Version: V4
Effective date: June 2026

1. Introduction

Coben Healthcare ("we", "us", "our") is committed to protecting the privacy and security of personal data. This Privacy Notice explains how we collect, use, store, and protect personal data relating to our employees, workers, and contractors, in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

This notice applies to:

- Current and former employees
- Workers and contractors
- Individuals engaged through temporary, locum, or assignment-based arrangements

It explains:

- What personal data we collect
- Why and how we use it
- The lawful bases we rely on
- How long we keep it
- Your rights under data protection law

2. Data Protection Principles

We process personal data in accordance with the UK GDPR data protection principles. This means that personal data will be:

- Processed lawfully, fairly, and transparently
- Collected for specified, explicit, and legitimate purposes
- Adequate, relevant, and limited to what is necessary
- Accurate and kept up to date
- Kept for no longer than necessary
- Processed securely to protect against unauthorised or unlawful processing, accidental loss, destruction, or damage
- Transferred internationally only in accordance with applicable legal safeguards

3. Types of Personal Data We Hold

We hold personal data in personnel files and secure HR, compliance, and IT systems. Depending on your role and engagement, this may include:

Personal and contact details

- Name, address, telephone number, email address
- Emergency contact / next of kin details
- Photograph

Personal characteristics and equality data

- Gender
- Marital status
- Disability or health information
- Race, ethnicity, religion (for equality monitoring purposes only)

Recruitment and engagement information

- CVs, covering letters, application forms
- Education and employment history
- References from previous employers
- Right-to-work documentation
- Professional registration and training records

Employment / engagement information

- Job title and role description
- Salary, fees, and payment details
- Terms and conditions of employment or engagement
- Appraisal, performance, supervision, and training records
- Disciplinary, grievance, or conduct records
- Sickness absence, family-related leave, and statutory leave records

Financial and statutory information

- National Insurance number
- Bank account details
- Tax code and payroll information

Security and systems data

- CCTV footage
- Building access card records
- Use of IT equipment, systems, internet, and telephones

Criminal conviction data

- DBS or equivalent criminal records checks where legally permitted and role-appropriate

4. How We Collect Your Data

We collect personal data directly from you during recruitment, onboarding, and throughout your employment or engagement.

We may also collect data from third parties where appropriate, including:

- Recruitment agencies
- Previous employers (references)
- Occupational health providers
- Professional bodies and regulatory authorities

Personal data is stored securely within our HR, compliance, and IT systems.

5. How We Use Your Data

We collect and use your personal data for the following purposes:

- Assessing your suitability for roles and assignments
- Managing your registration and onboarding
- Verifying your qualifications, experience, and right to work
- Matching you to appropriate roles with our clients
- Managing placements, compliance, and ongoing engagement
- Meeting legal and regulatory requirements

6. Lawful Bases for Processing

We process personal data only where permitted by law. The primary lawful bases we rely on include:

Activity	Lawful Basis
Managing employment or engagement contracts	Performance of a contract
Paying salary, fees, and expenses	Performance of a contract
Tax and National Insurance reporting	Legal obligation

Activity	Lawful Basis
Right-to-work checks	Legal obligation
Reasonable adjustments for disability	Legal obligation
Recruitment and placement decisions	Legitimate interests
Performance management and training	Legitimate interests
Attendance, conduct, and absence management	Legitimate interests
Personnel record keeping	Legitimate interests
Grievance and disciplinary procedures	Legitimate interests
Business planning, restructuring, and risk management	Legitimate interests
Preventing fraud and protecting systems	Legitimate interests
Providing references (where appropriate)	Legitimate interests

Our legitimate interests are balanced carefully against your rights and expectations.

7. Use of Digital and AI-Assisted Tools

As part of our recruitment, compliance, and placement processes, we may use digital tools, including AI-assisted systems, to help review CVs and professional information.

These tools are used solely to support professional judgement by assisting with:

- Consistency in CV and experience review
- Identification of relevant skills and experience
- Highlighting potential training or competency gaps
- Supporting safe and appropriate placement decisions

AI-assisted tools are advisory only. They do not make automated decisions about suitability, eligibility, or placement. All recruitment, compliance, and placement decisions are made by appropriately trained Coben Healthcare staff, taking account of additional information, discussion with individuals, and client or regulatory requirements.

These tools are used to help ensure individuals are placed safely, appropriately supported, and within their scope of practice.

8. Use of Third-Party Providers and Outsourcing

In some cases, we may use trusted third-party service providers to support our business operations. This may include administrative, compliance, IT, or recruitment support functions.

Some of these providers may be located outside the United Kingdom.

Where this applies:

- They act only on our instructions
- They are subject to strict confidentiality and data protection obligations
- We ensure appropriate safeguards are in place to protect your data

9. International Transfers

Where your personal data is transferred outside the United Kingdom, we ensure it is protected in accordance with UK GDPR.

This may include:

- Use of UK-approved International Data Transfer Agreements (IDTAs)
- Transfers to countries recognised as providing adequate protection
- Additional security measures where required

We take all reasonable steps to ensure your data remains secure when processed internationally.

10. Special Categories of Data

Special category data includes information relating to:

- Health
- Disability
- Race or ethnicity
- Religion or belief
- Sexual orientation
- Trade union membership
- Genetic or biometric data

We process special category data only where lawful and necessary, including:

- Equal opportunities monitoring
- Sickness absence management
- Determining reasonable adjustments
- Compliance with employment and health & safety obligations

The lawful bases relied upon include:

- Explicit consent (where required)
- Legal obligations
- Substantial public interest
- Information manifestly made public by you

11. Criminal Conviction Data

Criminal conviction data is collected only where legally permitted and relevant to the role. This is typically obtained during recruitment or onboarding.

We process this data to assess suitability or continued suitability for roles and rely on:

- Legal obligations
- Substantial public interest grounds

12. Failure to Provide Data

Failure to provide required personal data may mean we are unable to:

- Offer employment or assignments
- Comply with legal or regulatory obligations
- Administer pay, benefits, or placements

13. Who We Share Your Data With

Access to your data is restricted to staff who need it for legitimate business purposes and who are trained in data protection obligations.

We may share data with third parties where necessary, including:

- Clients (for placement and onboarding purposes in line with NHS requirements)
- Occupational health providers
- Payroll providers
- Professional or regulatory bodies
- Legal or regulatory authorities

We may also share data as part of a business sale, restructure, or where legally required. Data processing agreements are in place where required.

14. Data Security

We take appropriate technical and organisational measures to protect personal data against:

- Unauthorised access
- Loss or destruction
- Accidental disclosure

15. Data Retention

We retain personal data only for as long as necessary for its purpose.

Some data is retained for the duration of employment or engagement and for a period afterwards where required by:

- Law
- Regulatory obligations
- Legal claims or disputes

Retention periods are reviewed regularly to ensure compliance with data-minimisation principles.

16. Automated Decision-Making

Automated decision-making refers to decisions made using electronic systems without human involvement.

Coben Healthcare does not use automated decision-making for recruitment, suitability, compliance, or placement decisions. All such decisions involve human review and professional judgement.

Automated systems may be used for limited administrative purposes only, such as:

- Reminders for expiring documents
- Availability requests
- Internal CRM workflow support

These activities do not produce legal or similarly significant effects.

17. How Long We Keep Your Data

We retain your data only for as long as necessary to:

- Provide recruitment and placement services
- Meet legal and regulatory requirements
- Manage any potential legal claims

Retention periods are reviewed regularly.

18. Your Rights

You have the right to:

- Be informed about how your data is used

- Access your personal data
- Correct inaccurate data
- Request erasure in certain circumstances
- Restrict processing
- Data portability
- Object to processing
- Challenge automated decision-making

Requests can be made by emailing **GDPR@cobenhealthcare.com**

19. Consent

Where processing relies on consent, you may withdraw that consent at any time. This will not affect processing already carried out lawfully.

20. Complaints

If you believe your data protection rights have been breached, you may complain to:

Information Commissioner's Office
Wycliffe House, Water Lane
Wilmslow, Cheshire, SK9 5AF
Tel: 0303 123 1113

Document control

PP / v4 / June 2026