Staff and Other Partners Privacy Notice

Introduction

This privacy notice tells you what to expect when Conexus Healthcare CIC collects, uses and protects your personal information. It applies to all employees, casual workers, ex-employees, agency staff, self-employed contractors, secondees, apprentices, trainees, Directors and Non-Executive Board members, and other partners. The information we process about you will vary depending on your specific role and personal circumstances.

This notice should be read alongside our wider UK General Data Protection Regulation (UK GDPR) and IG policies and procedures. It is updated periodically and we will inform you of any significant changes.

The legal frameworks governing how we use your personal data include:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA 2018)
- Data (Use and Access) Act 2025
- Human Rights Act 1998
- Common Law Duty of Confidentiality
- NHS Codes of Confidentiality, Information Security and Records Management

Why we collect your information

As your employer or provider of other commissioned services, Conexus Healthcare needs to keep and process information about you for normal employment and contracting purposes. The information we hold and process will be used for our management and administrative purposes only. We will keep and use your data to enable us to run the business and manage our relationship with you effectively, lawfully and appropriately:

- During the recruitment or engagement process
- Whilst you are working for us or providing services to us
- For the duration of your service contract with us
- For a defined period after your employment or period of contracted work ends

This includes using information to enable us to comply with employment or other contracts; to meet legal requirements; pursue the legitimate interests of the organisation; and to protect our legal position in the event of legal proceedings. If you do not provide required data, we may in some circumstances be unable to comply with our obligations, and we will inform you of the implications of that decision.

What information we hold about you

The information we hold may include, but is not limited to:

- **Recruitment and starter information:** Application forms which may include your date of birth, gender, ethnicity, religion, home address, qualifications and telephone number.
- **Contract details:** For self-employed contractors, details of your address, office base, company registered number, and arrangements for commissioned services such as consultancy work.
- **Employment history:** Education and employment history including qualifications, right to work information, details of any declared criminal convictions, and details of any previous disciplinary action by another employer.
- **Identity documents:** A copy of your passport or similar photographic identification and/or proof of address documents (such as utility bills or bank statements).
- **References:** Names, addresses and job titles of your referees.
- **Contracts and correspondence:** Contracts of employment or commissioned services, including details about pay, start date and home address or place of work; correspondence with or about you relating to concerns, complaints, pay changes or role changes.
- **Payroll, benefits and expenses:** NI number, tax code, marital status, information about student loans, CCJs or court orders, company loans, overtime claims, bank account details, sort codes and invoices processed if self-employed.
- **Emergency contact details:** Next of kin addresses and telephone numbers.
- **Absence records:** Records of holiday, sickness and other absences including maternity, paternity, and compassionate leave.
- **Equal opportunities monitoring:** Religion, nationality and sexual orientation, collected in accordance with our equality monitoring policy.
- **Employment history with Conexus:** Training records, appraisals, performance measures, and where appropriate, disciplinary and grievance records.
- **Trade union membership:** For the purposes of deduction of subscriptions from salary.
- **Whistleblowing:** Details of any whistleblowing concerns raised by you, or to which you may be a party or a witness.
- **IT and CCTV monitoring:** Information derived from monitoring of IT equipment (for example use of smartcard to access clinical systems) or images/photographs from CCTV.
- **Declarations and agreements:** Confidentiality agreements; declarations of conflicts of interest, secondary employment, or gift declarations (which may also appear in annual accounts or reports).
- **Photographic ID:** For identification purposes and publicising your role on our public-facing website.
- **Health information:** Where necessary, we may hold information relating to your health including vaccinations and immunisations, sick leave forms, Fit to Work statements, reasons for absence, and GP reports and notes. This information is used to comply with our health and safety and occupational health obligations, to consider how your health affects your ability to do your job, and to administer statutory and company sick pay.

- **Accident and incident records:** Details of any accidents or incidents in the workplace, or where duties are undertaken on behalf of Conexus, including work risk assessments and visual display unit assessments.

Sources of Information

Much of the information we hold will have been provided by you directly. For employment purposes, some may come from other sources, including:

- Your manager or other internal sources
- NHS Jobs or a recruitment agency
- Your referees
- Security clearance providers such as the Disclosure and Barring Service (DBS)
- Your professional or registration body (to validate your professional registration as a clinician)
- Our Occupational Health provider or other health providers
- Pension administrators
- Government departments including HMRC
- Other organisations within the wider Conexus networks

Our Lawful Basis for processing your information

Personal Information

Under Article 6(1) of the UK GDPR, the lawful bases we rely on for processing personal information about you are:

- Article 6(1)(b) – Processing is necessary for the performance of a contract to which you are a party, or to take steps at your request before entering into a contract.
- Article 6(1)(c) – Processing is necessary to comply with a legal obligation, for example statutory reporting requirements or responding to lawful requests from courts or HMRC.
- Article 6(1)(e) – Processing is necessary for the performance of a task carried out in the public interest, namely the delivery of NHS commissioned healthcare services.
- Article 6(1)(f) – Processing is necessary for the purposes of our legitimate interests, for example to prevent fraud, for administrative purposes, or to report potential crimes, provided your interests or fundamental rights do not override those interests.
- Article 6(1)(a) – Consent, where you have provided explicit agreement for specific uses of your data.

Special Categories of Personal Data

Where we process special categories of personal data (such as health information, racial or ethnic origin, religious beliefs, sexual orientation, trade union membership, or biometric data), we do so only where a condition under Article 9 of the UK GDPR applies, most commonly:

- Article 9(2)(b) – Processing necessary for carrying out our obligations in the field of employment, social security or social protection law.

- Article 9(2)(h) – Processing necessary for the purposes of occupational medicine and assessment of your working capacity.
- Article 9(2)(a) – Where you have given explicit consent, which you have the right to withdraw at any time.
- Article 9(2)(c) – Processing necessary to protect your vital interests in an emergency.

In limited cases we may ask for your explicit consent. Where we do, you have the right to withdraw that consent at any time; this will not affect the lawfulness of any processing that took place prior to withdrawal.

Automated decision-making

Some of our HR systems and tools may use automated processing to assist in decision-making, for example in areas such as rostering or recruitment screening. Where any such processing produces decisions that have a significant effect on you, we will ensure appropriate safeguards are in place in accordance with applicable data protection legislation, including the Data (Use and Access) Act 2025. You have the right to request human review of any such decision, to express your point of view, and to contest decisions made about you.

Who we may share your information with

Other than as set out below, we will only disclose information about you to third parties if we are legally obliged to do so or where we need to comply with our contractual duties to you. We may transfer information about you to other organisations for purposes connected with your employment or the management of the organisation's business. These may include:

- Our external payroll provider
- Our HR advisors
- Pension or health insurance scheme administrators
- Primary Care Networks on behalf of which you may be providing services
- NHS Jobs or recruitment agencies (for recruitment-related purposes)
- Government departments such as HMRC, where legally required
- The Disclosure and Barring Service (DBS) or other security clearance providers
- Occupational Health providers
- Professional or registration bodies
- Law enforcement or courts where legally required

We will also share work-related information about staff in a public-facing or senior role in response to Freedom of Information or similar requests, and may have to disclose information about staff numbers and types of work undertaken. Personal details will not be shared in these circumstances.

Information relating to prospective applicants will be held on the NHS Jobs portal or via the relevant recruitment agency. Conexus Healthcare will only hold personal information on candidates who have been shortlisted and invited to interview (as well as those of the successful candidate). Any information used for monitoring purposes will be anonymised where possible.

International transfers of data

In limited and necessary circumstances, your information may be transferred outside of the UK or to an international organisation to comply with our legal or contractual requirements. Where this happens, we ensure a similar degree of protection is afforded by using transfer mechanisms approved under UK data protection law, such as:

- UK adequacy regulations
- The UK International Data Transfer Agreement (IDTA)
- The UK Addendum to the EU Standard Contractual Clauses

We will always inform you if your data is transferred outside of the UK and the safeguards in place.

How we keep your information secure

We are committed to protecting your privacy and will only use your information collected lawfully in accordance with the UK GDPR, the Data Protection Act 2018, and all applicable NHS guidance. Specifically, we:

- Maintain appropriate technical and organisational security measures to protect your data from accidental loss, unauthorised access, alteration or disclosure
- Limit access to your personal data to those employees, agents, contractors and other third parties who have a genuine business need to see it
- Require all employees and sub-contractors to sign a confidentiality agreement
- Hold data securely on our Conexus systems and use an external IT provider to ensure that data is backed up regularly
- Put in place appropriate data processing agreements (under Articles 24-28 UK GDPR) with any sub-contractor or third party that acts as a data processor on our behalf
- Have procedures in place to deal with any suspected data security breach, and will notify you and any applicable regulator where we are legally required to do so

Every member of staff who works for an NHS organisation or in an NHS-commissioned organisation has a legal obligation to keep information about patients and colleagues confidential.

CCTV

We employ surveillance cameras (CCTV) on and around our sites in order to:

- Protect staff, visitors and organisational property
- Apprehend and prosecute offenders and provide evidence for criminal or civil court action
- Provide a deterrent effect and reduce unlawful activity
- Help provide a safer working environment
- Monitor operational and safety-related incidents

You have the right to make a Subject Access Request of surveillance information recorded of yourself. Requests should be directed to the IG Lead using the contact details in this notice, and you will need to provide sufficient information to identify you and help us locate the relevant images. We reserve the right to withhold information where permissible under UK GDPR and will only retain surveillance data for a reasonable period, or as long as is required by law.

How long we keep your information

Any records we hold will be kept in line with the NHS Records Management Code of Practice for Health and Social Care, which sets out how long different types of records are retained. Details of the specific retention periods that apply to your records are available on request using the contact details below.

Further information on records retention can be found at:
https://transform.england.nhs.uk/information-governance/guidance/records-management-code/

Your rights

Under the UK GDPR and Data Protection Act 2018, you have the following rights in relation to your personal data. We will seek to deal with any request without undue delay and in any event within one calendar month (although we may extend this period in certain complex cases, in which case we will notify you):

Right	What This Means
Right of Access	You have the right to request a copy of the personal data we hold about you (Subject Access Request). There is no charge for this.
Right to Rectification	You have the right to request that we correct inaccurate or incomplete data we hold about you.
Right to Erasure	In certain circumstances, you have the right to request that we delete your personal data. Note that this is not an absolute right in employment contexts.
Right to Object	You have the right to object to processing based on legitimate interests. We will review each objection carefully.
Right to Restrict Processing	You may request that we limit the processing of your data in certain circumstances, for example while we investigate an objection.
Right to Data Portability	You have the right to receive a copy of your data in a structured, commonly used and machine-readable format.
Right to Withdraw Consent	Where processing is based on consent, you may withdraw that consent at any time. This will not affect the lawfulness of prior processing.

Right to Human Review	You have the right to request human review of any automated decision that has a significant effect on you, and to contest such decisions.

Accessing the information we hold about you

To submit a Subject Access Request (SAR), or to exercise any of the rights set out above, please contact us in one of the following ways:

- By email: wyicb-wak.conexussar@nhs.net
- By post: IG Lead, Conexus Healthcare CIC, C/O Sandal Castle Medical Centre, Asdale Road, Wakefield, WF2 7JE

To help us locate your records efficiently, please include your full name, date of birth, home address, and a description of your request. There is no charge for accessing the information we hold about you.

Identity and contact details of the Data Controller and Data Protection Officer

Conexus Healthcare CIC is the data controller of your personal data for the purposes of the UK GDPR and the Data Protection Act 2018 (as amended, including by the Data (Use and Access) Act 2025).

If you have any initial enquiries regarding this notice, your data, or if you require further information on the data held by Conexus, please contact the IG Lead:

- Email: wyicb-wak.conexuscontact@nhs.net
- Post: IG Lead, Conexus Healthcare CIC, C/O Sandal Castle Medical Centre, Asdale Road, Wakefield, WF2 7JE

For questions relating to how we process your data or UK GDPR rules in general, please contact our Managing Director or our Data Protection Officer:

Contact	Details
Managing Director	Steve Knight - Email: steve.knight1@nhs.net
Data Protection Officer	Helen Holt - Email: Helen.Holt@this.nhs.uk Post: The Health Informatics Service, Unit 13 Ainley Industrial Estate, Ainley Bottom, Elland, HX5 9JP

Making a complaint about how we use your personal data

If you are unhappy with the way we have handled your personal data, you have the right to make a complaint to us. We take all data protection complaints seriously and have a clear process in place to deal with them. You can make a complaint by:

- Emailing the IG Lead using the contact details above
- Writing to us at the postal address above

To help us deal with your complaint efficiently, please include your name and contact details, a description of your concern, and any relevant dates or reference numbers.

When we receive your complaint, we will acknowledge it within 30 days. We will then investigate your concerns, take appropriate steps to address them, and inform you of the outcome without undue delay. Raising a data protection complaint will not disadvantage you in any way in your employment or engagement with us.

If you are still unhappy following our response, you have the right to lodge a complaint with the UK supervisory authority, the Information Commissioner's Office (ICO), although we would encourage you to contact us first so we have the opportunity to put things right:

Information Commissioner's Office (ICO)

Address: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Tel: 0303 123 1113

Website: https://ico.org.uk Complaints: https://ico.org.uk/make-a-complaint

Changes to this privacy notice

We may amend this privacy notice from time to time to reflect changes in our practices or applicable law. Any updates will be published on our website and shared with staff. If you are dissatisfied with any aspect of this notice, please contact the IG Lead.

Updated June 2026