Data Protection & Privacy Policy

Nationwide Care Recruitment

This notice explains how we collect, use, disclose, retain and protect personal information when providing temporary healthcare staffing and recruitment services to private care homes, private hospitals, community care services, NHS organisations and other health and social care providers, and when individuals use our website or contact us.

1. Who We Are

Nationwide Care Recruitment (company number 11862776), trading as Nationwide Care Recruitment ("Nationwide Care Recruitment", "we", "us" or "our"), is registered in England and Wales. Our registered office is 5 Brayford Square, London, England, E1 0SG

For most recruitment, workforce, employment/engagement, compliance, website and business-administration activities described in this notice, we act as a data controller. In some circumstances, particularly where a healthcare client instructs us to process personal information solely on its behalf, we may act as a data processor. The relevant contract or data processing agreement will determine the parties' roles.

Privacy and data protection enquiries may be sent to:

info@nationwidecarerecruitment.co.uk

Telephone: 0161 871 0962.

Where legislation requires us to appoint a Data Protection Officer, we will publish the DPO's contact details. Otherwise, references in this notice to our Data Protection Lead mean the person responsible for overseeing our data protection compliance.

2. Scope of This Notice

This notice applies to personal information relating to:

- temporary workers, agency workers, nurses, healthcare assistants, support workers, care staff, domestic/support staff and other healthcare professionals who register or work with us;
- job applicants and prospective candidates;
- employees, self-employed contractors and other individuals engaged by us, where relevant to the external-facing privacy information in this notice;
- representatives, employees and contacts at client organisations, including private care homes, hospitals, community care providers, NHS trusts/organisations and other health and social care bodies;
- referees, emergency contacts and other third parties whose details are supplied to us;
- suppliers, professional advisers and business contacts; and

- visitors to our website, people who submit enquiries, and recipients of our communications.

This website notice may be supplemented by more specific privacy information at the point personal information is collected, for example candidate registration forms, worker privacy notices, client contracts or recruitment portals.

3. Data Protection Law

We process personal information in accordance with applicable UK data protection and privacy law, including the UK General Data Protection Regulation ("UK GDPR"), the Data Protection Act 2018 ("DPA 2018"), the Data (Use and Access) Act 2025 ("DUAA"), and the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR"), as amended from time to time.

We apply the data protection principles of lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability.

4. Personal Information We Collect

4.1 Candidates, workers and healthcare professionals

- identity and contact information, including name, title, address, telephone number, email address, date of birth, photograph and emergency contact details;
- CV, employment history, skills, professional experience, availability, preferred roles, locations, shift information and assignment history;
- identity and right-to-work evidence, immigration/status information and share-code verification information where applicable;
- professional registration and regulatory information, including NMC or other registration details, PIN/registration status, restrictions or conditions where relevant;
- qualifications, training, competencies, mandatory training records, professional development and occupational requirements;
- references, referee details and information obtained during employment-history and suitability checks;
- Disclosure and Barring Service (DBS) information and other criminal-offence information where lawful and necessary for regulated healthcare work;
- health, disability, vaccination, immunisation, occupational health, reasonable-adjustment or fitness-to-work information where necessary and lawful;
- equality, diversity and monitoring information where collected lawfully, usually on a restricted-access basis;
- payroll, tax, National Insurance, bank/payment and pension information where relevant;
- timesheets, attendance, cancellations, performance, supervision, complaints, incidents, safeguarding concerns, investigations, disciplinary/contractual action and clinical-governance information;
- communications with us, including emails, messages, call records/recordings where used and notes of conversations;
- driving licence, vehicle, insurance or travel information where relevant to an assignment; and
- technical information generated when using our website, systems, apps or portals.

4.2 Client organisations and business contacts

- name, job title, employer/organisation, business address, telephone number and email address;
- booking, rota, staffing, service and contractual information;
- communications, meeting notes, complaints, incident information and service feedback;
- billing, purchasing and payment information; and
- information necessary for safeguarding, quality assurance, audit, regulatory compliance or the management of an assignment.

4.3 Service users, patients and residents

Our core business is supplying staff, not creating or maintaining patient or resident records. However, limited information about a service user, patient or resident may be provided to us or recorded by us where necessary to investigate or manage an incident, complaint, safeguarding matter, medication concern, clinical-governance issue, worker performance issue, legal claim or regulatory matter.

Such information may include health information and other highly sensitive data. We seek to minimise it, restrict access, use it only for the relevant purpose, and avoid retaining clinical information that is not necessary for our role. The care provider/NHS organisation will normally remain controller of its clinical records.

4.4 Website and digital information

- IP address, device and browser information, approximate location derived from IP, log data and security information;
- pages visited, interactions and referral information;
- information submitted through online forms, email links or recruitment portals; and
- cookie and similar-technology information, subject to applicable consent requirements.

5. How We Obtain Personal Information

- directly from you through registration, application, onboarding, telephone, email, forms, interviews, meetings, portals and ongoing communications;
- from healthcare clients and placement providers in connection with bookings, assignments, feedback, incidents, safeguarding or quality matters;
- from referees, former employers, training providers, professional bodies and regulators;
- from DBS checking/umbrella services, right-to-work verification services and identity-verification providers;
- from occupational health or other compliance providers where appropriate;
- from recruitment platforms, job boards, professional networking sites and publicly available professional sources;
- from government, regulatory, law-enforcement or safeguarding bodies where lawful; and
- automatically through our website, IT systems, security logs and cookies.

6. Why We Use Personal Information and Our Lawful Bases

We identify and document an appropriate lawful basis before processing personal information. The basis depends on the purpose and circumstances and may include contract, legal obligation, legitimate

interests, recognised legitimate interests where the statutory conditions are met, consent, vital interests, or public task where applicable.

Purpose	Typical Article 6 basis	Examples
Recruitment and registration	Contract / steps before contract; legitimate interests	Assess applications, communicate with candidates, verify experience, match workers to roles.
Worker engagement and assignments	Contract; legal obligation; legitimate interests	Manage availability, bookings, timesheets, pay, performance, supervision and assignment records.
Compliance and safer recruitment	Legal obligation; legitimate interests; recognised legitimate interests where applicable	Right-to-work, professional registration, training, references, DBS/safeguarding and fraud-prevention checks.
Client service delivery	Contract; legitimate interests	Fill shifts, provide compliant worker profiles, manage bookings and client relationships.
Safeguarding, incidents and clinical governance	Legal obligation; legitimate interests; vital interests; recognised legitimate interests where applicable	Investigate concerns, protect service users, cooperate with clients/regulators, maintain safe staffing.
Legal and regulatory matters	Legal obligation; legitimate interests	Respond to regulators, courts, law enforcement, HMRC, Home Office, safeguarding authorities and professional bodies.
Business administration and security	Legitimate interests; legal obligation	IT security, fraud prevention, audits, insurance, accounting, debt recovery and legal claims.
Direct marketing	Consent or legitimate interests where PECR and data protection law permit	Relevant business-to-business communications and candidate/service updates; opt-out rights always apply.
Website analytics/non-essential cookies	Consent where required by PECR	Analytics, advertising or other non-essential technologies.

Where we rely on legitimate interests, we consider the purpose, necessity and impact on individuals and implement safeguards. Where a recognised legitimate interest under current law applies, we will use it only within the statutory conditions.

7. Special Category Personal Information

Healthcare recruitment can require us to process special category information, including health, disability, racial or ethnic origin, religious beliefs, trade union membership, biometric data used for unique

identification, and information about sex life or sexual orientation where such information is lawfully collected.

We will only process special category information where both an Article 6 lawful basis and an Article 9 condition apply. Depending on the purpose, relevant Article 9 conditions may include employment, social security and social protection law; health or social care; reasons of substantial public interest; legal claims; vital interests; or explicit consent where consent is genuinely appropriate.

Where the DPA 2018 requires an additional Schedule 1 condition and/or an Appropriate Policy Document, we will satisfy and document those requirements. Access to special category information is restricted to personnel who need it.

8. Criminal Offence and DBS Information

Because many healthcare roles involve regulated activity or work with vulnerable people, we may process criminal conviction, offence, allegation, barring and DBS information. We do so only where authorised by law and where the processing is necessary and proportionate for the relevant role or safeguarding purpose.

We apply the additional safeguards required by Article 10 UK GDPR and the DPA 2018, including relevant Schedule 1 conditions and an Appropriate Policy Document where required. DBS certificate information is handled securely, disclosed only to authorised persons, and retained only for as long as necessary in accordance with applicable DBS and data protection requirements.

9. Automated Decision-Making and Profiling

We may use technology to help search, filter, rank or match candidates against objective role requirements. We do not intend to make solely automated decisions that produce legal or similarly significant effects on individuals unless permitted by law and appropriate safeguards are in place.

Where a significant decision is made solely by automated means, we will provide the information and safeguards required by applicable law, including relevant rights to obtain human involvement, make representations or contest a decision where those rights apply.

10. Who We Share Personal Information With

Where necessary, proportionate and lawful, we may share personal information with:

- private care homes, private hospitals, community care providers, NHS trusts/organisations, integrated care bodies and other healthcare clients seeking temporary staffing;
- professional regulators and registration bodies, including the Nursing and Midwifery Council where relevant;
- DBS/umbrella bodies, identity, right-to-work, compliance, training and occupational-health providers;
- referees, former employers and qualification/training providers;
- payroll, pension, accounting, banking and payment service providers;

- our recruitment, rostering, CRM, LMS, cloud, communications, IT support, cyber-security, document-management and data-hosting suppliers;
- insurers, auditors, solicitors, professional advisers, debt-recovery providers and other parties involved in establishing, exercising or defending legal claims;
- local authorities, safeguarding teams, CQC or other health/social-care regulators where applicable, NHS bodies, HMRC, the Home Office, police, courts and other public authorities where required or permitted by law;
- a purchaser, investor, funder or successor in connection with a genuine corporate transaction, subject to appropriate confidentiality and data protection safeguards; and
- other parties where you direct us to share information or where you have provided valid consent and consent is the appropriate basis.

We do not sell personal information. We require processors acting on our behalf to use personal information only on documented instructions, keep it secure, maintain confidentiality and assist us with applicable data protection obligations.

11. Healthcare Client Disclosures and Data Minimisation

To enable a client to assess and book a worker, we may provide an appropriate worker profile containing information such as name, role, relevant experience, qualifications, training/compliance status, professional registration status and availability. We do not routinely disclose copies of identity documents, DBS certificates, health information or other highly sensitive records unless disclosure is necessary, lawful, proportionate and appropriately secured.

Clients receiving worker information are expected to use it only for legitimate recruitment, placement, safeguarding, workforce and regulatory purposes and to comply with their own controller obligations.

12. International Transfers

Some technology, cloud or service providers may store or access personal information outside the United Kingdom. Before making a restricted international transfer, we assess whether the transfer rules apply and use a lawful transfer mechanism.

Where appropriate, this may include UK adequacy regulations/data bridges, the UK International Data Transfer Agreement (IDTA), the UK Addendum to the EU Standard Contractual Clauses, or another lawful safeguard or derogation. Where required, we carry out a transfer risk assessment and apply supplementary technical, contractual or organisational measures.

13. Data Security and Confidentiality

We use proportionate technical and organisational measures designed to protect personal information. These may include:

- role-based access controls and least-privilege access;
- strong authentication, password controls and multi-factor authentication where supported;
- encryption in transit and at rest where appropriate;

- secure cloud, email, document and recruitment systems;
- device management, anti-malware, patching, backups, logging and monitoring;
- confidentiality obligations and staff training, including phishing and data-breach awareness;
- supplier due diligence and data processing agreements;
- secure disposal and deletion procedures;
- incident response and business-continuity arrangements; and
- periodic review of access, risks, systems and data protection controls.

No system can guarantee absolute security. We therefore use risk-based controls and review them as technology, threats and our processing activities change.

14. Personal Data Breaches

We maintain procedures for identifying, containing, assessing, documenting and responding to personal data breaches. Where a breach is likely to result in a risk to individuals' rights and freedoms, we will notify the Information Commissioner as required by law. Where the risk is high, we will also notify affected individuals unless a lawful exception applies.

Workers, staff and contractors must report suspected loss, unauthorised disclosure, misdirection, cyber incident or other data breach to us immediately through our internal reporting route.

15. Data Protection by Design, DPIAs and Accountability

We build data protection considerations into new systems, projects and processing activities. We conduct Data Protection Impact Assessments (DPIAs) where processing is likely to result in a high risk to individuals, including where required for new technologies, systematic monitoring, significant automated decision-making or large-scale/sensitive processing.

We maintain appropriate records of processing, contracts, retention arrangements, security measures, lawful-basis decisions, legitimate-interest assessments and other accountability documentation where required.

16. How Long We Keep Personal Information

We keep personal information only for as long as necessary for the purpose for which it was collected, including legal, regulatory, safeguarding, contractual, insurance, tax, accounting and dispute-resolution requirements. Retention may differ according to the record and circumstances.

Record category	Typical approach
Candidate registration / recruitment records	Kept while the candidate is active and for an appropriate period afterwards based on recruitment, limitation, regulatory and business requirements.
Unsuccessful / non-engaged applicant records	Normally retained for a limited period, commonly around 6–12 months, unless there is a documented reason or consent to retain longer.

Worker assignment, compliance, contract and payment records	Generally retained for the engagement and an appropriate post-engagement period, commonly up to 6 years where needed for contractual/legal claims, with longer retention where law or an active matter requires it.
Tax, payroll and accounting records	Retained for the statutory period applicable to the relevant record.
DBS / criminal-record information	Certificate information is retained only for the minimum period necessary; limited check/status and recruitment-decision records may be retained where lawful and required.
Safeguarding, incident, complaint, investigation and regulatory records	Retained according to the seriousness of the matter, legal/regulatory requirements, limitation periods, safeguarding needs and any ongoing investigation or claim.
Website enquiries	Retained only as long as needed to respond and manage the resulting relationship or legal/business record.
Marketing records	Until consent is withdrawn/objection made or the information is no longer needed, with suppression records retained as necessary to honour opt-outs.
Cookie/analytics information	According to the cookie type and duration stated in our cookie settings/policy.

Our internal retention schedule sets more specific periods. We may retain information for longer where necessary for safeguarding, a complaint, litigation, regulatory action, fraud prevention or another legal reason. When information is no longer required, we securely delete, destroy or anonymise it.

17. Your Data Protection Rights

Depending on the circumstances, you may have rights to:

- be informed about how your personal information is used;
- request access to personal information we hold about you;
- request correction of inaccurate or incomplete information;
- request erasure where the legal conditions are met;
- request restriction of processing in certain circumstances;
- object to processing based on legitimate interests and object at any time to direct marketing;
- request data portability where the legal conditions apply;
- withdraw consent at any time where processing relies on consent, without affecting earlier lawful processing; and
- exercise rights relating to certain automated decisions and profiling.

These rights are not absolute. Exemptions or restrictions may apply, for example where we must retain information to comply with law, protect safeguarding interests, preserve legal privilege or establish, exercise or defend legal claims.

To exercise a right, contact data@nationwidecarerecruitment.co. We may request proportionate information to verify identity. We normally respond without undue delay and within the statutory time

limit. Where permitted by law for a complex or multiple request, the response period may be extended and we will explain this.

18. Direct Marketing

We may send service, recruitment or business communications where permitted by UK GDPR and PECR. Marketing consent will be obtained where required. Where legitimate interests may lawfully be used, we will consider individuals' reasonable expectations and privacy rights.

You can opt out of marketing at any time by using an unsubscribe facility where provided or contacting us. Service, compliance, safeguarding, assignment and contractual communications are not marketing and may continue where necessary.

19. Cookies and Similar Technologies

Our website may use strictly necessary cookies and, subject to applicable consent requirements, analytics, functionality, advertising or other non-essential cookies. Non-essential cookies will not be set before valid consent where PECR requires consent.

Our cookie banner or consent-management tool should provide clear choices to accept or reject non-essential cookies and allow preferences to be changed. More detail should be provided in a separate Cookie Policy or cookie settings panel, including cookie names, purposes, providers and durations.

20. Children

Our recruitment and staffing services are not directed at children. We do not knowingly recruit individuals below the lawful age for the roles we supply. We may incidentally process limited information about children in safeguarding, emergency-contact or service-user contexts where lawful and necessary, in which case enhanced care and data minimisation apply.

21. Accuracy and Your Responsibilities

Please keep information supplied to us accurate and up to date, particularly contact details, right-to-work status, professional registration, training, health/fitness information relevant to work, and other compliance information. If you provide personal information about another person, you must have an appropriate basis to do so and, where appropriate, make them aware that their information has been provided to us.

22. Complaints

If you have concerns about our use of personal information, please contact our Data Protection Lead first so that we can investigate and respond.

You also have the right to complain to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection. Current contact and complaint information is available at ico.org.uk. The

ICO can also be contacted by telephone on 0303 123 1113 or by post at Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

23. Changes to This Policy

We review this policy at least annually and sooner where our services, systems, suppliers, legal obligations, regulatory guidance or processing activities materially change. The current version will be published on our website with its effective date. Where a change materially affects how we use personal information, we will take reasonable steps to bring it to the attention of affected individuals.

24. Contact Us

Data Protection Lead
Nationwide Care Recruitment

Email: info@nationwidecarerecruitment.co.uk
Telephone: 0161 871 0962

Legislative and Regulatory Reference Points

This policy has been drafted with reference to the UK GDPR, Data Protection Act 2018, Data (Use and Access) Act 2025, PECR and current Information Commissioner guidance as at 22 July 2026. It should be reviewed against future legislative changes and updated ICO guidance.