PRIVACY POLICY
AUGUST 2023

NDR SERVICES (UK) LIMITED
Registration Number: 08938819 Registered in England & Wales
Registered Office: 32 Elizabeth Street, Corby, Northants, NN17 1PN

What is a Privacy Notice?
A privacy notice is a statement explaining how personal and confidential information about candidates, corporate clients, visitors, and staff is collected, used and shared within NDR Services (UK) Ltd (referred to as "We, "Our" or "Us") Different organisations use different names for privacy notices, and it can sometimes be referred to as a privacy statement, a fair processing notice or a privacy policy.

What is NDR and what does it do?
NDR is a local based Recruitment agency specialising in manufacturing and logistics roles, across Northamptonshire, Cambridgeshire & Leicestershire.
Everything NDR does is underpinned by our core values:

- Candidate Experience
- Collaborative partnerships
- Transparency
- Relentless innovation
- Human centred

Why have a privacy notice for candidates, corporate clients, visitors, and staff?
NDR would like to demonstrate its commitment to openness and accountability. We recognise the importance of protecting personal and confidential information in all that we do to ensure that we meet our legal responsibilities and other duties, including compliance with the following:

- Data Protection Act (DPA)
- General Data Protection Regulation (GDPR)
- Computer Misuse Act
- Human Rights Act
- Copyright Design and Patents Act
- ISO 9001:2015 Quality Management System

How we collect your information?
Your information could be collected in several ways by us. This maybe through our services, for example job applications, on the website, on social media, or in person, for example on the phone or in branch. Or from third-party job boards where you have registered your Curriculum Vitae (CV) for the purposes of finding work.

What information do we collect about you?
The information that we collect is provided by you and may include details such as:

Personal information

- name, address, telephone, email date of birth and next of kin
- copies of driving licence, passport, and proof of current address, such as bank statements and council tax bills
- evidence of how you meet the requirements of a job, including CV and reference checks
- evidence of your right to work in the UK and immigration status
- bank details, tax and NI number for processing payments
- other information relevant to customer surveys and/or offers
- Guest / visitors to one of your sites

Special Category information

- Diversity and equal opportunities monitoring information – this can include information about your race or ethnicity, religious beliefs, sexual orientation, disability
- Information about your health, including any medical needs or conditions

For some jobs we maybe require to ask you to;

- provide person information of individuals who can provide references
- provide details of any criminal convictions (including a DBS certificate or update service details)

Why do we collect information?

We collect personal and confidential information about you to support you in the recruitment and employment process. It is important that we provide the best experience while meeting your needs.

How do we use your information and why is this important?

We use your personal information to deliver the best experience to help understand your and where it is necessary to meet our obligations which may include:

- to provide a recruitment service to you and to facilitate the recruitment process
- to assess data about you against vacancies which we believe may be suitable for you
- to send your information to clients in order to apply for jobs, to assess your eligibility for jobs or to process you for work (including pre-contract, during and post-contract)
- to improve our client and recruitment experience and to make our services more valuable to you (including gathering your feedback and tailoring our website, applications and our group companies' websites when you log on to enrich your personal online experience)
- to respond to questions and enquiries
- To engage third parties where we have retained them to provide services that we, you or our client have requested including payroll services, references, qualifications and criminal reference checking services, verification of the details you have provided from third party source, psychometric evaluation or skill tests
- To inform third parties, regulatory or law enforcement agencies if we believe in good faith that we are required by law to disclose it in connection with the detection of crime, the collection of taxes or duties, in order to comply with any applicable law or order of a court of competent jurisdiction, or in connection with legal proceedings. Please also note we may retain and share details of incidents where threats have been made to the safety and security of our members of staff with any law enforcement agencies when needed. This may also result in individuals being barred from using our services
- To use your information on an anonymised basis to monitor compliance with our equal opportunities policy

How do we keep your information safe and maintain confidentiality?

The GDPR and Data Protection Act has strict principles governing our use of information and our duty to ensure that it is kept safe and secure. Your information may be stored using electronic or paper records, or a combination of both. All our records are restricted so that only authorised individuals have access to them. Restricted access might be using technology or other environmental safeguards.

Sharing with other organisations

Personal information you provide to us will be made available to clients and our processors. By providing your information to us you have agreed to our terms and conditions that you have

consented through the sign-up process. Implied consent under certain conditions maybe applied for example:

- Applying directly to jobs via independent jobs boards (candidates or staff)
- Processing information for the purpose of processing payments (salary)

We will share your information to other agencies or organisations who are involved in the recruitment process, who may be the data controller and/or processor of your information.
We may be required to share your personal information for "Legitimate interests" which may include (but not limited to):

- To assess your information about you with current vacancies which we believe may be suitable for you
- To send your information to clients in order to apply for jobs, to assess your eligibility for jobs or to process you for work (including pre-contract, during and post-contract)
- To engage third parties where we have retained them to provide services that we, you or our client have requested including payroll services, references, qualifications and criminal reference checking services, verification of the details you have provided from third party source, psychometric evaluation or skill tests
- Third parties to whom we may choose to sell, transfer or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as we currently do, which can also extend to consents for marketing communications
- To inform third parties, regulatory or law enforcement agencies i required by law to disclose it in connection with the detection of crime, the collection of taxes or duties, in order to comply with any applicable law or order of a court of competent jurisdiction, or in connection with legal proceedings.
- To use your information on an anonymised basis to monitor compliance with our equal opportunities policy
- To improve our customer service and to make our services more valuable to you (including gathering your feedback via email and tailoring our website, applications and our group companies' websites when you log on to enrich your personal online experience)

Audit, Research, and Artificial Intelligence ("AI")

Audit
Mandatory audits are undertaken to ensure we are process, store and share your data appropriately. We are unable to apply data opt-outs to audits as these are mandatory and regulatory requirements.

Research
We will share your anonymised information for statistical analysis. Once the data has gone through the anonymised process it will no longer be classified as personal information and is exempt from GDPR & the Data Protection Act. We are unable to apply data opt-outs as the data would not be able to identify a specific individual.

Artificial Intelligence ("AI")
We are always looking at ways to innovate to improve our efficiency to delivery you the best experience. AI maybe used in the future and if we are to use your information where you are formally identified then we ask for your consent.

We may use anonymised data for the use of AI as this will no longer be classified as personal information and is exempt from GDPR & the Data Protection Act. We are unable to apply data opt-outs as the data would not be able to identify a specific individual.

Do you have the right to withhold or withdraw your consent for information sharing?
You have the right to refuse (or withdraw) consent to your information being shared at any time. This may be referred to as 'opt-out'. If you choose to prevent your information being disclosed it may restrict the services we provide to you, which may mean we may not be able to use our services. The possible consequences of withholding your consent will be fully explained to you at the time should this situation occur.

Where do we store your information?
NDR securely stores your information electronically and occasionally in paper form. We use different systems depending on the process we require to undertake and are subject to change:
Sage - Specialist software for managing payroll services
Orange HRM – Specialist Software for managing Recruitment Services.
Formidable – A service used in our online registration process.

How long we keep information about you?
Your personal data will be kept in line with statutory and recommend retention periods:

Statutory record retention period

Record type	Statutory retention period
Accident books, accident records/reports	3 years from the last entry (or until any younger person involved in the accident reaches 21).
Accounting records	3 years for private companies, 6 years for public limited companies.
Coronavirus furlough records	6 years for furlough records including amounts claimed, claim period per employee, reference number and calculations. For flexible furlough - usual and actual hours worked.
First aid training	6 years after employment.
Fire warden training	6 years after employment.
Health and Safety representatives and employees' training	5 years after employment.
Income tax and NI returns, income tax records and correspondence with HMRC	Not less than 3 years after the end of the relevant financial year.
Medical records and details of biological tests under the Control of Lead at Work Regulations	40 years from the date of the last entry.
Medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry.

Medical records under the Control of Asbestos at Work Regulations	40 years from the date of the last entry (medical records); 4 years from the date of issue (medical examination certificates).
Medical records under the Ionising Radiations Regulations 1999	Until the person reaches 75 years of age, but in any event for at least 50 years.
National minimum wage records	6 years after the end of the pay reference period following the one that the records cover.
Payroll wage/salary records (also overtime, bonuses, expenses)	6 years from the end of the tax year to which they relate.
Records of tests and examinations of control systems and protective equipment under the Control of Substances Hazardous to Health Regulations (COSHH)	5 years from the date on which the tests were carried out.
Records relating to children and young adults	until the child/young adult reaches the age of 21.
Retirement Benefits Schemes	6 years from the end of the scheme year in which the event took place.
Statutory Maternity Pay records including Mat B1s (also shared parental, paternity and adoption pay records)	3 years after the end of the tax year in which the maternity period ends.
Subject access request (SAR)	1 year following completion of the request.
VAT deferral (COVID-19)	6 years.
Working time records including overtime, annual holiday, time off for dependents, etc	2 years from date on which they were made.

Recommended retention period	
Record type	Statutory retention period
Actuarial valuation reports	Permanently.
Collective agreements	6 years after the agreement ends.
CCTV footage	ICO retention practice is 6 months following the outcome of any formal decision or appeal. CCTV footage may be

	relevant to a disciplinary matter or unfair dismissal claim
Driving offences	Must be removed once the conviction is spent under the Rehabilitation of Offenders Act 1974.
Flexible working requests	18 months following any appeal. This is because a further request cannot be made for 12 months following a request plus allowing for a 6 month tribunal limitation period on top.
Inland Revenue/HMRC approvals	Permanently.
Money purchase details	6 years after transfer or value taken.
Parental leave	18 years from the birth of the child
Pension records	12 years after the benefit ceases.
Pension scheme investment policies	12 years from the ending of any benefit payable under the policy.
Personnel files and training records (including disciplinary and working time records)	6 years after employment ceases but may be unreasonable to refer to expired warnings after two years have elapsed.
Recruitment application forms and interview notes (for unsuccessful candidates)	6 months to a year. Because of the time limits in the Equality Act, relating to advertising of vacancies and job applications should be at least 6 months. A year may be more advisable as the time limits for bringing claims can be extended. Successful job applicants' documents will transfer to the personnel file.
Redundancy details, calculations of payments, refunds	6 years from the date of redundancy.
References	Outgoing references given by an organisation should be retained for at least one year after the reference is given to meet the limitation period for potential defamation claims. However, employers may be able to justify a longer retention period of six years, if they are concerned about defending any future claims. For incoming references received from previous employers, organisations could simply retain a note that satisfactory references were received. For references of unsuccessful applicants, a retention period of nine months to a year is probably justified, because the time limit for discrimination is six months plus possible time limit extensions. Some employers may decide they have no need to keep

	references for new staff once the employee has successfully completed a probationary period.
Right to work in the UK checks	Home Office recommended practice is 2 years after employment ends.
Senior executives' records (senior management team or equivalents)	Some records may need permanent retention such as documents from the company's incorporation, shareholdings, resolutions, memorandum and articles, annual returns, register of directors interests, share documents, accounts, liability policies, pension scheme documents etc most of which should be retained permanently. Retain personal records, performance appraisals, employment contracts etc for 6 years after the employee has left to reflect the main limitation period.
Statutory Sick Pay (SSP) records, calculations, certificates, self-certificates, occupational health reports. Also COVID-19-related SSP records such as the dates off sick.	Six months after the end of the period of sick leave is sensible in case of a disability discrimination claim. For personal injury claims, the limitation is 3 years. If there's a contractual claim for breach of an employment contract then keep records for 6 years after the employment ceases. Employers should keep a record of SSP paid due to COVID-19 as HMRC may request records.
Termination of employment, for example early retirement, severance or death in service	At least 6 years although the ICO's retention schedule suggests until employee reaches age 100.
Terms and conditions including offers, written particulars, and variations	Review 6 years after employment ceases or the terms are superseded.
Time cards	2 years after audit.
Trade union agreements	10 years after ceasing to be effective.
Trust deeds and rules	Permanently.
Trustees' minute books	Permanently.
Works council minutes	Permanently.

Your records which have reached the end of their administrative life must be destroyed in as secure a manner as is appropriate to the level of confidentiality or protective markings they bear. The methods used to destroy records must provide adequate safeguards against the accidental loss or disclosure of the contents.

A record of the destruction of records, showing their reference, description and date of destruction should be maintained and preserved by the department responsible for the records so that the

organisation is aware of those records that have been destroyed and are therefore no longer available.

What are your rights?
You have the right to confidentiality under Data Protection Law, the Human Rights Act 1998 and the Common Law Duty of Confidentiality

The right to be informed – you have the right to know what information we hold about you, what we use it for and if the information is shared, who it will be shared with. We do this through this privacy notice.

The right of access – to information held about you. For further information please refer to the section "How can you gain access to the information that we hold about you?"

The right to rectification – this is your right to have your personal data rectified if it is inaccurate or incomplete. If you believe that the information recorded about you is incorrect, you will need to tell us by contacting your personal representative. We will correct factual mistakes and provide you with a copy of the corrected information.

The right to erasure – this is also known as your 'right to be forgotten' where there is no compelling reason to continue processing your data in relation to the purpose for which it was originally collected or processed. Parts of your records must remain in line "Statutory record retention period". It is extremely rare that we destroy or delete records earlier than the "Recommended retention period".

The right to restrict processing – this is your right to block or suppress the processing of your personal data. For example: if you would like to restrict processing of your information from marketing then you can do this by completing a SAR (Subject Access Request)

The right to data portability – this is your right to obtain and re-use any information you have provided to us as part of an automated process. At present we do not process any personal data that meets this requirement.

The right to object – this is your right to object to us processing your data. Whilst we will stop processing your data it may mean we are unable to provide a service to you. We are obligated to keep your data in line "Statutory record retention period".

Rights in relation to automated decision making and profiling – GDPR provides safeguards for individuals against the risk that a potentially damaging decision would be taken without human intervention. While we may use systems to determine how suited an individual is for a role, it does not replace decisions made by us. We use this to improve your experience when using our services.

If you have provided your consent, you have the right to withdraw your consent at any time by contacting us.

You have the right to lodge a complaint with the Information Commissioner Office (ICO) if you believe that the we have not complied with the requirements of the GDPR or the DPA with regards

to your personal data. Please refer to the section, “How can you contact us with queries or concerns about this privacy notice?” or “How can you make a complaint?”

How can you gain access to the information we hold about you?
Under the General Data Protection Regulations (GDPR) and Data Protection Act, you have the right to request access to the information that we hold about you using the process known as a ‘Subject Access Request’ (SAR).

If you would like a copy of your records, we hold you are able to submit a request via email to support@ndr-services.co.uk

* **A request for a copy is free, however we may charge an administrative fee if you require more than a single copy of your information**

How can you contact us with queries or concerns about this privacy notice?
If you have any queries or concerns regarding the information that we hold about you or have a question regarding this privacy notice, then please contacts us:
Post: NDR Services (UK) Ltd, 32 Elizabeth Street, Corby, Northants, NN17 1PN
Email: support@ndr-services.co.uk
Telephone: 0800 246 5376

How can you make a complaint?
You have the right to make a complaint if you feel unhappy about how we hold, use or share your information. We would recommend that you contact us initially to talk through any concerns that you may have:
Post: NDR Services (UK) Ltd, 32 Elizabeth Street, Corby, Northants, NN17 1PN
Email: support@ndr-services.co.uk
Telephone: 0800 246 5376

If you remain dissatisfied following the outcome of your complaint, you may then wish to contact the Information Commissioner’s Office:

- Post: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
- Web: Information Commissioner
- Telephone: 0303 123 1113