RECRUITMENT PRIVACY NOTICE

We are the JD Group (we/us/our). We'd like to tell you how we use your personal information when we collect it as part of the recruitment process, such as:

- when you're talking to us about applying for a job
- when we're reviewing a job application that you've sent to us or which has been sent to us on your behalf
- when you're going through the assessment and interview process with us
- where you're taking the steps necessary to enter into a contract of employment with us, if you're successful with your application.

You should also read this privacy notice if you're engaged within a contract for services process.

We are committed to keeping your personal information safe, complying with our obligations under data protection law and being open with you about how and why we process your personal information.

Where do we collect your data from?

We collect your data as part of the recruitment process when you, or someone authorised by you, provides us with your personal data. This includes the following sources:

- **You** – when you apply for a vacancy that we place on our website or elsewhere
- **Recruitment agency** – where you have registered with or authorised a recruitment agency to provide us with your CV, job application or profile so that you can apply for a role with us
- **Social media** – where you have made information available on a social media site (such as LinkedIn)
- **Referees** – individuals who you tell us can provide references about you, to help us determine your suitability for a role
- **Background check agencies** – organisations that can provide us with information about any criminal convictions that you may have, which may be needed for us to determine your suitability for a role
- **Job boards and talent acquisition platforms** – organisations that host information about our current vacancies and with whom you apply for jobs and provide your personal information to.

What information do we collect and what is it used for?

The table below sets out the types of personal data that we collect, what our lawful basis is for collecting and processing it and how long we keep it for before permanently erasing it:

Description of data	Personal data collected	Lawful basis / purpose	Retention period*
General contact information	Name, address, contact details such as email	Legitimate interests: to conduct our recruitment process and communicate with you. You can choose how we	

	address and phone number, date of birth	contact you e.g. email or SMS. You can change your preferences when you wish. If you choose SMS and change your mind, you can unsubscribe at any time We also use this information to form a contract of employment between us if an offer is made and accepted	16 months
Education background	Schools attended, grades achieved, qualifications and training	Legitimate interests: to assess your suitability for a role	
Employment history	Previous and current employer(s), job title(s), and salary, reference	Legitimate interests: to assess your suitability for a role	
Interview scores	Notes, test scores, aptitude test results	Legitimate interests: to assess your suitability for a role	
Immigration status	Citizenship, visa status, passport (or other ID document)	Legal obligation: so that we can ensure that we are legally able to employ you without breaching immigration law	
Disabilities	Any disabling or other medical conditions	Legitimate interests: so that we can comply with obligations to make reasonable adjustments (e.g. for an interview process)	
Equality data	Ethnic origin, gender, sexual orientation, religious information	Legitimate interests, consent: to ensure that we are meeting our obligations under equality laws, and monitoring diversity within our workforce. In some cases, we will ask for your consent to collect this information. **This information is not in any way linked to our assessment of your application**	

**Please note that if you are recruited, this retention period will change to that which is set out in our Employee Privacy Notice. Your personal data will then be included within our People systems and processed in accordance with our Employee Privacy Notice.*

More about background checks

We carry out background checks for all colleagues after they have accepted a role. The type of check conducted is dependent on the role and the business area, however, the process may conclude after your start date. All offers of employment are subject to satisfactory references and, where relevant, a Disclosure and Barring Service (DBS) check. Standard reference checks involve obtaining a minimum of 12 months of employment history (the maximum is 5 years for management/senior roles) which are conducted by our People Operations team centrally. We may use trusted third parties to carry out checks on our behalf.

If you are offered a permanent role following a period working as an agency worker within one of our Distribution Centres, we will obtain confirmation of your engagement with the agency as part of the onboarding process via our People Operations and Relations teams.

All roles at airport stores are subject to enhanced screening which includes a DBS check. These are completed by in-store management teams in line with each airport body's guidelines. Roles which involve working with children are also subject to DBS checks.

How do we protect your information?

The information we process is always kept secure. We store your personal data in our cloud-based Applicant Tracking System (ATS). The data is stored in encrypted form and is only ever accessible to specific authorised individuals within the People Team who require access to the data to carry out their duties. We also hold information within our internal IT systems.

All our teams are trained in handling personal data, and we have appropriate policies and procedures in place to ensure and monitor compliance.

Who do we share your data with?

We share some of your personal information with third parties. These include referees, organisations that provide us with background checks – including criminal record checks where required – and organisations that provide us with various business services. In certain circumstances, we may also share some of your personal information with companies that provide training programmes and deliver our Traineeship Programmes. In addition, we will sometimes be required to share your personal data with relevant authorities where we are required by law to do so.

We share information only with those organisations who have also put in place similar safeguards, to ensure that your data is kept securely and in compliance with data protection laws.

Your data may be held outside of the country in which you live. In addition, your personal data may sometimes be transferred to and stored in a country outside the United Kingdom or the European Economic Area. In such cases, we ensure that we have appropriate safeguards (including contractual obligations with those third parties) in place to protect your personal data.

How long do we hold your data for?

If your application is unsuccessful, we hold your data for a maximum period of up to 16 months. This is for the following reasons:

- In case the offer to a successful candidate falls-through, and we want to make an appointment from the existing applications
- In case a similar or related vacancy arises, and we would like you to consider applying for it
- In case we need to bring or defend any legal claims or handle complaints which may require use of your personal data
- To enable us to comply with certain legal reporting obligations such as the NI Equal Monitoring requirements (where applicable)

As the retention period approaches, we will contact you to ask if you'd like us to retain your details for a further 12 month period, for example if a similar vacancy was to arise. This is entirely your choice and we will only keep the data for longer than the usual retention period if you ask us to. If not, we will securely and permanently erase it from our records and systems.

If your application is successful, your data will then be held in line with our Employee Privacy Notice which you will be able to review as soon as your employment with us has begun.

What are your rights?

You have the following rights, in respect of your personal data, under data protection law:

- The right to access your personal data
- The right to object to our purposes for processing your personal data
- The right to have inaccurate personal data corrected
- The right to ask us to stop processing your personal data
- The right to ask us to delete your personal data
- The right to withdraw consent (where our processing of your personal data is based upon your consent)
- The right to complain to the data protection regulator

To exercise any of these rights or to raise any queries about our processing of your personal data, please contact: dataprotectionofficer@jdplc.com

For further information about your personal data more generally, you can contact your local data protection regulator. If you wish to make a complaint to your local regulator, about how we have handled your personal data, then you may do so, however, we would welcome the opportunity to discuss your complaint with you first to see if it can be resolved. In some cases, the regulator may expect you to raise a complaint with us first before submitting a complaint to them. You can check your local EU regulator here: Our Members | European Data Protection Board (europa.eu)

In the UK, the data protection regulator is the Information Commissioner's Office (ICO), and their details are available from www.ico.org.uk