Candidate Privacy Notice

Version 1.0 on publication | Effective **12 October 2026** | Next review October 2027

1. About this notice

This notice explains how Northdoor plc collects and uses personal information about people who apply to work with us, whether as an employee, contractor or agency worker, and people who send us a speculative application or are put forward by a recruitment agency. It covers the whole process, from application to the point we make an offer or close your application.

If you join us, our Employee Privacy Notice will explain how we use your information during your employment. For other uses of our website, see our Privacy and Cookie Notice.

2. Who we are

Northdoor plc is the controller of your information. We are registered in England and Wales under company number 02192480, and our registered office is Third Floor, Bentima House, 168 to 172 Old Street, London EC1V 9BP. We are registered with the Information Commissioner's Office (ICO) under registration number ZA056094.

Contact us about data protection
Email: data.controller@northdoor.co.uk
Post: The Data Protection Lead, Northdoor plc, Third Floor, Bentima House, 168 to 172 Old Street, London EC1V 9BP
Telephone: 020 7448 8500

For questions about a vacancy or your application, or to ask for an adjustment to the process, contact our HR team at **recruitment@northdoor.co.uk**.

3. The information we collect

Category	Examples
Identity and contact	Name, address, email address, telephone number
Application	Your CV and covering letter, employment history, qualifications, skills, certifications and professional memberships, and anything else you choose to tell us
Terms	Current and expected salary and benefits, notice period, preferred working pattern and location
Assessment	Interview notes, technical test and assessment results, and our hiring decision and the reasons for it
Right to work and identity	Passport, visa or share code details, and other documents that prove your identity, address and right to work in the UK
References and checks	References from previous employers, verification of qualifications and employment history, and, for some roles, credit or security clearance results
Criminal records	The outcome of a Basic DBS check, and any information you choose to disclose about unspent convictions
Adjustments	Information about a disability or health condition you share so that we can adjust the process for you

We are an equal opportunities employer. We do not ask about your ethnicity, religion, sexual orientation or other protected characteristics, and you do not need to include them in your CV.

4. How we use your information and our lawful basis

Data protection law requires us to have a lawful basis for each use of your information. These are set out below.

Purpose	Lawful basis
Assessing your skills and experience against the role, shortlisting, interviewing and deciding whom to appoint	Legitimate interests (recruiting the right people); steps taken at your request before entering into a contract
Communicating with you about your application and the process	Legitimate interests; steps before a contract
Making an offer and preparing your contract	Steps before a contract
Checking your right to work in the UK	Legal obligation
Taking up references and verifying your qualifications and employment history	Legitimate interests (making sure candidates are suitable for roles with privileged access to client systems)
Basic DBS check and any further screening a client requires before granting access to its systems	Legitimate interests; contract with our client. See section 5 for the additional conditions
Making reasonable adjustments to the process	Legal obligation (Equality Act 2010). See section 5
Dealing with complaints and legal claims, including discrimination claims	Legitimate interests; legal obligation

If you do not provide information we need, such as proof of your right to work, we may not be able to progress your application or make you an offer.

5. Sensitive information

Some of the information above is special category data (information about health or disability) or criminal records data. The law protects it more strongly, and we use it only where an extra condition applies:

- **Adjustments for disability or health:** the employment condition in Schedule 1, Part 1, paragraph 1 of the Data Protection Act 2018.
- **Criminal records:** the employment condition in Schedule 1, Part 1, paragraph 1. Our people have privileged access to the systems of banks and insurers. Where a client must screen outsourced staff under its own regulatory requirements, we also rely on the regulatory requirements condition in Schedule 1, Part 2, paragraph 12.

Our Data Protection Policy includes the appropriate policy document that explains how we protect this information and how long we keep it. We do not ask about criminal records until we have made a conditional offer. You do not need to tell us about spent convictions unless the role is exempt under the Rehabilitation of Offenders Act 1974, and we will tell you if it is. A criminal record will not automatically prevent you working with us; we consider whether it is relevant to the role. We ask about health only where needed to make adjustments, or after an offer where the role requires it.

6. Automated decisions and AI

We do not make recruitment decisions based solely on automated processing, and we do not use artificial intelligence or automated tools to shortlist, score or reject candidates. Every application is read and assessed by a person.

If you apply through LinkedIn, LinkedIn may use its own automated tools, for example to match or rank applicants. These are controlled by LinkedIn, not by us. LinkedIn's privacy policy, at linkedin.com/legal/privacy-policy, explains how it uses your information.

7. Where we get your information

Most information comes directly from you. We also receive information from:

- LinkedIn, where we advertise most of our roles, when you apply through it or send us your profile;
- recruitment agencies that put you forward, where we use them;
- colleagues who refer you to us;
- the referees you name, and former employers and education providers who confirm your history;
- the Disclosure and Barring Service, through the Basic DBS certificate you apply for yourself on GOV.UK and show us, and, for some roles, credit reference agencies and government vetting bodies; and
- the Home Office online right to work service, using a share code you give us.

We will not contact referees or start background checks without telling you first, and normally only after we have made a conditional offer.

LinkedIn is a separate controller for the information you give it, including your profile and anything you submit through its job application tools. Once your application reaches us, this notice applies to our copy.

8. Who we share your information with

Your application is received and held by our HR and Office Manager, and shared only with the hiring manager and interviewers, by encrypted email. We do not sell your information. We share it outside Northdoor only where needed:

Recipient	Why
Microsoft (Microsoft 365 and Outlook)	To receive and store applications by email; acts as our processor under a written contract
Egress	To send applications securely to hiring managers by encrypted email; acts as our processor under a written contract
Recruitment agencies	To manage applications they put forward to us
Our clients	Where a role needs access to a client's systems and the client vets people first. We will tell you before we share anything, and share only what the client needs
Referees and former employers	To obtain and verify references, after telling you
Professional advisers, regulators, courts and the Home Office	Where the law requires, or to deal with a complaint or legal claim

9. International transfers

Applications are held in Microsoft 365 and Egress, which store our data in the UK or European Economic Area. If a supplier needs to access it from elsewhere, we protect the transfer using UK adequacy regulations, the UK Extension to the EU to US Data Privacy Framework, or the UK International Data Transfer Agreement or UK Addendum, with a transfer risk assessment. You can ask us for details.

10. How long we keep your information

Information	How long
Applications that are not successful, including speculative applications	6 months after we tell you our decision, so that we can respond to any questions or claims. The emails and any copies are then deleted
Applications that lead to an offer	Moved to your personnel file and kept as our Employee Privacy Notice explains
Right to work records for people who join us	For the duration of employment and 2 years after it ends, as the law requires
DBS certificate information	We record that a check was done and the outcome, and do not keep a copy of the certificate beyond 6 months

When information is no longer needed, we delete or anonymise it securely.

11. How we protect your information

We are certified to ISO/IEC 27001 for information security management. Applications are held in a mailbox that only our HR and Office Manager can access, protected by multi-factor authentication, and are shared with hiring managers only by Egress encrypted email. Hiring managers delete their copies once a decision is made.

12. Your rights

You have the right to:

- **access** a copy of the personal information we hold about you;
- **rectification** of information that is wrong or incomplete;
- **erasure** of your information in certain circumstances;
- **restrict** our use of your information in certain circumstances, for example while we check its accuracy;
- **object** to our use of your information where we rely on legitimate interests;
- **data portability**, meaning to receive information you gave us in a machine-readable format, where we process it by automated means on the basis of consent or contract; and
- **withdraw consent** at any time where we rely on it, without affecting what we did before you withdrew.

To exercise any right, email data.controller@northdoor.co.uk. We may ask you to confirm your identity. We will respond within one month, which we may extend by up to two further months for complex requests; if we do, we will tell you why within the first month. There is normally no charge.

13. How to complain

If you are unhappy with how we have handled your information, please contact us first at data.controller@northdoor.co.uk. We will acknowledge your complaint within 30 days, investigate it without undue delay, keep you informed and tell you the outcome.

If you remain unhappy, you can complain to the Information Commissioner's Office: ico.org.uk/make-a-complaint, telephone 0303 123 1113, or write to Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

14. Changes to this notice

We review this notice at least once a year and when we change how we recruit. The version number and effective date at the top show when it last changed.