



Privacy Notice for Job Applicants

In order to comply with our contractual, legal and management obligations and responsibilities, we process personal data of applicants in relation to an application for employment.

1. Processing Personal Data

The term 'processing' includes the initial collection of personal data, the holding and use of such data, as well as access and disclosure, through to final destruction.

NFP assumes the role of data controller in the processing of personal data obtained through our services. We are committed to safeguarding your privacy and ensuring that your personal information is handled responsibly, transparently, and in compliance with the data protection law.

Any access to personal data is limited to only those that need to process the data and those who need to see relevant data in relation to your application.

Data is processed as follows:

- **Legitimate Interest:** Information is provided by you either via a CV or application form and in answer to our interview questions, where relevant. Relevant personal data processed as a result of you providing it represents a legitimate interest on our part to process your application of employment.
- **Legal Obligations:** To comply with our legal obligations, a right to work check (which includes ethnic origin and racial data, along with our requirement to see your passport) is completed if you are successfully appointed.

All such data will be processed in accordance with UK Data Protection Law and this NFP Privacy Notice, as amended from time to time.

If your application is successful, this will include processing sensitive personal data in relation to any offer of employment. Details of this processing will be provided with any offer of employment. Our Privacy Statement for employees will apply from the point of any offer onwards.

Data We collect.

The categories of data for job applicants that we process means any information about an individual from which that person can be identified. It does not include data where the identity has been removed i.e., anonymised data. Examples of the categories of personal information we may process about you include:

Personal and contact details such as name, address, National Insurance number Nationality / right to work information, qualifications, previous experience, referees, and answers to questions relevant to the role.



2. Purpose of Processing

- Personal data is used to communicate with job applicants throughout the recruitment process. This includes sending application acknowledgments, scheduling interviews, providing updates on the status of their application, and making job offers.
- To assess suitability for appointment to a particular post
- For administration and management purposes, to satisfy any regulatory requirements and carrying out appropriate security checks.
- Where the post is offered and accepted, to enter the employment contract.
- For employment checks after an offer has been made including those required to confirm identity; establish trustworthiness, integrity, and reliability.
- To check an employee's entitlement to work in the UK/Ireland; and, where necessary, to carry out criminal records checks to ensure that individuals are permitted to undertake the role in question.

We may use external recruitment platforms to identify potential candidates. Your personal details, as entered by you, will be stored on this system.

We carry out due diligence on all our third-party suppliers to ensure they process data in compliance with data protection legislation.

3. How your information is stored

Data will be stored in a range of different places depending on its nature and purpose, including, in human resource information systems, and in other IT systems, such as Outlook, Egnyte and SharePoint. NFP reserve the right to store your data in the USA, or any country in the world that it deems appropriate; we are a multinational corporation, and our systems may integrate with NFP Corp's global systems, as appropriate. An example of this would be UKG, who have datacenters in other countries, including France, India, Singapore, and Canada, where your data may be sub-processed if required. Please note that data transferred between the NFP's European and USA offices is protected by the Standard Contractual Clauses adequacy measure. NFP will only process your data where sufficient data protection measures have been put into place to ensure that your data is secure and compliantly processed.

4. Data Retention

All data is retained for 12 months from the point of application. After this time, your data is securely destroyed, and very limited information is retained electronically for internal reporting reasons only. This is simply your name, date of application, role applied for, whether it was a direct application or via a third party and, if so, the name of that party and the outcome of your application.



If you choose to actively remain on our lists to be notified of future recruitment opportunities, your data will be retained in line with this. Data will be deleted periodically to comply with our data retention requirements.

5. Disclosure and Barring

The successful applicant where their role requires them must agree to a Basic Disclosure under the Disclosure and Barring Service (DBS) for UK applicants and to the National Vetting Bureau (NVB) for Ireland. Employment will be offered to the successful applicant subject to a satisfactory Disclosure report.

Applicants must disclose any charge or conviction, whether current or pending, which may affect their suitability for the position advertised. This clause is subject to current relevant restrictions in force in respect of spent convictions and exemptions under the Disclosure and Barring Service (DBS) procedures.

Any information disclosed during the dv process which is not relevant to the application will be destroyed and relevant information will be held until the conclusion of the recruitment process and, if the candidate is not successful, will be destroyed when they are informed that their application has been unsuccessful.

If you would like to view a copy of our policy on recruitment of ex-offenders, then please email

nfpeurhr@nfp.co.uk

6. Your rights in relation to your data

- You have the right to access your personal data. A subject access request can be made to **HR** by sending an email to nfpeurhr@nfp.co.uk
- You have a right to be informed. NFP is obliged to provide you with details of the collection and use of the data they collect about you.
- You have the right to have your personal data rectified if it is inaccurate or incomplete.
- You have the right to have your personal data deleted or removed if there is no reason for its continued storage and processing.
- You have the right to object to having your data processed. If we believe there is a legitimate business reason for continuing this, we will discuss this with you.
- You have a right to ask that your data be transferred to another designated controller in a commonly acceptable and easily readable digital format. However, this is applicable only when the processing of said information relies on either (i) your consent or (ii) the execution of a contract to which you are a party.
- You have a right to be included in decisions made entirely by automated processes i.e., without any human involvement in which case you have a right to object to such processing.
- You have a right to complain to the Information Commissioners Office (ICO), details below.

Further details about GDPR and your rights under GDPR can be found on the ICO's website at <https://ico.org.uk>