



WILLIAM JACKSON FOOD GROUP

CANDIDATE PRIVACY NOTICE

1. What is the purpose of this document?

The William Jackson Food Group is a "controller". This means that we are responsible for deciding how we hold and use personal data about you. You are being provided with a copy of this privacy notice because you are applying for work with us (whether as an employee, worker or contractor). It makes you aware of how and why your personal data will be used, namely for the purposes of the recruitment exercise, and how long it will usually be retained for. It provides you with certain information that must be provided under data protection legislation.

2. The kind of information we hold about you

In connection with your application for work with us, we will collect, store, and use the following categories of personal data about you:

- The information you have provided to us in your curriculum vitae and covering letter.
- The information you have provided on our application form including name, address, telephone number, email address, employment history and qualifications.
- Information we obtain pursuant to the recruitment process (for example, through any tests or recruitment exercises you complete).
- Any information you provide to us during an interview.
- Information obtained from third parties to verify any information you have told us (such as information in relation to your employment history from any references you have provided).

We may also collect, store and use the following types of more sensitive personal data:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
- Information about your health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences.

3. How is your personal data collected?

We collect personal data about candidates from the following sources:

- You, the candidate.
- Disclosure and Barring Service in respect of criminal convictions.
- Recruitment agencies we use from time to time.
- Your named referees.
- Third parties who undertake any part of the recruitment process on our behalf.
- Publicly accessible sources.

4. How we will use information about you

We will use the personal data we collect about you to:

- Assess your skills, qualifications, and suitability for the role.
- Carry out background and reference checks, where applicable.
- Communicate with you about the recruitment process.
- Keep records related to our hiring processes.
- Comply with legal or regulatory requirements.

It is in our legitimate interests to decide whether to appoint you to the relevant role since it would be beneficial to our business to appoint someone to that role.

We also need to process your personal data to decide whether to enter into a contract of employment with you.

Having received your CV and covering letter and/or your application form, we will process that information to decide whether you meet the basic requirements to be shortlisted for the role. If you do, we may ask you to undertake further tests or recruitment exercises to see if you are suitable for the role. We will then decide whether your application (and the results of any tests and recruitment exercises where applicable) are strong enough to invite you for an interview. If we decide to call you for an interview, we will use the information you provide to us at the interview to decide whether to offer you the role. If we decide to offer you the role, we will then take up references and/or carry out a criminal record and any other checks notified to you before confirming your appointment.

If you fail to provide information when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we will not be able to process your application successfully.

5. How we use particularly sensitive personal data

We will use your particularly sensitive personal data in the following ways:

- We will use information about your disability status to consider whether we need to provide appropriate adjustments during the recruitment process.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

6. Information about criminal convictions

Depending on the role, we may need to process information about criminal convictions if we would like to offer you the role (conditional on checks and any other conditions, such as references, being satisfactory). We are entitled to carry out a criminal records check in order to satisfy ourselves that there is nothing in your criminal convictions history which makes you unsuitable for the role. For example, if the role requires a high degree of trust and integrity (e.g. if it involves dealing with customer money) we may ask you to seek a basic disclosure of your criminal records history.

7. Automated decision-making

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making.

8. Data sharing

We will only share your personal data the following third parties for the purposes of processing your application:

- You may be asked to submit your information to us via a third party recruitment platform. If you are asked to do this such third party may ask you to agree to their terms and conditions and may act as a controller in respect of any personal data submitted through their recruitment platform. In such circumstances we recommend that you review such third party's terms and conditions and privacy policy and ensure that you are happy to agree to such terms before submitting any personal data to that third party.
- Third parties who undertake any testing or recruitment exercises on our behalf (you will be informed of such third parties before you undertake such tests or recruitment exercises).

- Other entities in the William Jackson Food Group. All William Jackson Food Group companies are required to take appropriate security measures to protect your personal data in line with our policies.

If you are appointed to the role your personal data will be shared in accordance with our Employee Privacy Statement which will be provided to you on your appointment to the role.

9. Data security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need-to-know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

10. Data retention

If you are successful, your personal data will be retained in accordance with our retention policy, a copy of which is available on request.

If you are unsuccessful we will retain your personal data for a period of 6 months after we have communicated to you our decision. We retain your personal data for that period so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way. After this period, we will securely destroy your personal data in accordance with applicable laws and regulations.

If you have submitted your personal data through any third party recruitment platform that acts as a controller, that third party will retain your personal data in accordance with its retention policy.

If we wish to retain your personal data on file, on the basis that a further opportunity may arise in future and we may wish to consider you for that, we will write to you separately, seeking your explicit consent to retain your personal data for a fixed period on that basis.

11. Rights of access, correction, erasure, and restriction

Under certain circumstances, by law you have the right to:

- Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have exercised your right to object to processing (see below).
- Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal data for direct marketing purposes.
- Request the restriction of processing of your personal data. This enables you to ask us to suspend the processing of personal data about you, for example if you want us to establish its accuracy or the reason for processing it.
- Request the transfer of your personal data to another party.

If you want to review, verify, correct or request erasure of your personal data, object to the processing of your personal data, or request that we transfer a copy of your personal data to another party, please contact the Data Champion in writing.

12. Data Champion

We have appointed a Data Champion to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal data, please write to: The Data Champion at privacy@wjfg.co.uk. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.