

Staying Vigilant Against Recruitment Scams

We have noticed an increasing trend whereby individuals are being targeted by scammers posing as representatives of Macfarlane Packaging/Group, offering fake job opportunities. This issue has been particularly prominent in the USA (note that we are primarily a UK/Europe-based company and very rarely hire in the USA).

Scammers often impersonate legitimate recruiters, employers, or job placement agencies, advertising fake job vacancies via email, text messages, and WhatsApp. They may even pretend to be specific employees of our company to deceive job seekers into providing money or personal information.

If you are contacted about an interview or job offer from Macfarlane, it will always be through an official email address (our email format is {first initial of first name/full last name}@macfarlanepackaging.com). First contact almost always comes via our central recruitment team, this will usually be to arrange a local interview at one of our sites or to have a direct preliminary conversation with you either on the phone or via video/MS Teams. At no point in the recruitment process will we ever request any form of payment or bank details, even if you are applying from overseas.

While we do use social media channels to share news and updates about job opportunities (primarily LinkedIn), we never seek to formalise interview arrangements or extend job offers (or ask for personal information) via these platforms. We also do not communicate with candidates through WhatsApp and rarely use SMS. If an SMS is sent, it will be part of an ongoing recruitment process, and we will never ask for personal information through this medium. So, if you receive a suspicious text, please contact your recruiter for verification.

Whilst Microsoft Teams is often used for preliminary video-interviewing, again, we would never make a job-offer without going on to meet a candidate in person at one of our sites.

For details on how we handle personal data, visit: https://macfarlanepackaging.com/privacy-policy

If you suspect you have been a victim of a scam involving the Macfarlane name, please always contact us directly at <u>careers@macfarlanepackaging.com</u>

Common Signs of Recruitment Scams:

- **Opportunities 'too good to be true'**: Be cautious of job offers that promise high pay for minimal work or no experience.
- Unprofessional Communication: Scammers may use personal email addresses, contain spelling and grammatical errors, or send unprofessional-looking documents.
 Emails may come from unofficial addresses that do not match our corporate standards.



- Upfront Payment Requests: Legitimate employers do not ask for money upfront. Be wary of fees for background checks, training, or equipment... or any mention of bank-details/financial transactions
- Requests for Personal Information: Do not provide sensitive personal data early in the job application process. Scammers may ask for documents like passports or bank details.
- **Rushed Hiring Process**: Offers made without an interview or after an unusually quick process could indicate a scam.
- **Selling/purchasing items**: We never ever sell merchandise, phones, or laptops to candidates.

How to Protect Yourself:

- Research: Verify the company and individuals involved. Firstly, check our official
 vacancies page: https://macfarlanepackaging.com/careers/vacancies If a job is not
 listed here, it is most likely not genuine (as all our vacancies are updated here
 regularly and in real time)
- **Protect Personal Information**: Only share sensitive information once you have verified the company's legitimacy and received a formal job offer.
- **Contact Directly**: If in doubt, reach out to us using contact details from our official website (<u>careers@macfarlanepackaging.com</u>), not those provided in a suspicious job ad or email.
- Trust Your Instincts: If something feels off, it probably is. Trust your gut.

*Please share this information with your network to help protect against employment scams. For more details, visit Employment Fraud | Action Fraud.

What to Do if You Think You've Been targeted:

- Take a screenshot or note of the scammer's details and report them to Action Fraud.
- If you have given money, contact your bank immediately.
- Alert the website or social media platform where you were contacted to inform them of the fraudulent activity.

Resources/Key Contacts in reporting recruitment fraud

- National Crime Agency Fraud
- Action Fraud (National Reporting Centre for Fraud and Cybercrime)
- Jobs Aware (SAFERJobs)