
Privacy policy

UNION MARKETING | EFFECTIVE DATE: 1 JANUARY 2026

Draft for business verification. Read the owner review note on the final page before publication.

1. Who we are and how to contact us

Union Marketing ("we", "us" or "our") operates unionmarketing.org.uk and provides outsourced sales and face-to-face marketing services. We are the controller of personal information used for our own website enquiries, business relationships and recruitment.

Privacy contact: Union Marketing, 103 Union Street, London, SE1 0LA, United Kingdom.

Email: admin@unionmarketing.co.uk

Telephone: 0203 343 1041.

This notice explains our intended handling of personal information under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and applicable electronic communications rules. It covers website visitors, people contacting us, applicants and business contacts. Separate workforce and campaign notices apply where more specific information is needed.

2. Information we collect

Enquiries and business contacts: your name, email address, telephone number, organisation, role, correspondence and information you choose to provide about a proposed service or relationship.

Applicants: contact details, CV, work and education history, qualifications, availability, interview notes and relevant references. Where necessary at the appropriate stage, we may request evidence of identity and permission to work.

Website use: technical information processed by hosting or security services, which may include IP address, browser and device details, access times, requested pages and error or security logs. Optional tracking is subject to section 6.

Preferences and administration: communication preferences, consent and objection records, and relevant contract, invoice and payment records when doing business with you.

3. Where information comes from

We obtain information directly when you email, telephone, apply or otherwise contact us, and through website operation. If an agency, referrer, referee, client or public professional source supplies information about you, we will identify that source and the relevant categories in the information we give you. We provide this within the applicable legal period, normally within one month and sooner if we first contact you or disclose the information.

How we use information

PURPOSES, LEGAL BASES & YOUR CHOICES

4. Purposes and lawful bases

Answering enquiries: our legitimate interest in responding to questions and managing communications. Where you ask us to take necessary steps towards a contract with you personally, we rely on those pre-contractual steps.

Providing services: performance of a contract with you personally; for contacts at corporate clients and suppliers, our legitimate interest in delivering services and managing the business relationship.

Recruitment: necessary steps towards an employment or engagement contract you request, and our legitimate interest in assessing suitability and administering a fair recruitment process. Mandatory eligibility checks rely on the applicable legal obligation. Future-opportunity retention requires your separate consent.

Website security: our legitimate interest in maintaining reliable services, identifying misuse and protecting information. Optional analytics or advertising technologies, if introduced, rely on consent under this policy.

Records, disputes and legal duties: legal obligations for required tax, accounting or regulatory records; legitimate interests for proportionate complaint handling and establishing, exercising or defending legal claims.

Marketing: consent for promotional email or text to individuals unless a valid statutory exception applies. Relevant messages to corporate business contacts may rely on legitimate interests where electronic marketing rules permit. Each promotional message will identify us and offer an easy way to opt out.

Where we rely on legitimate interests, we consider necessity, your reasonable expectations and the effect on your rights. We do not use that basis where your interests or fundamental rights override ours.

5. Your choices and required information

You may object to direct marketing at any time. Email our privacy contact or use the unsubscribe option. We will stop that use, including related profiling. We may retain minimal suppression details to respect your choice.

You can withdraw consent at any time by contacting us, without affecting the lawfulness of earlier processing. Giving us an enquiry or application does not itself mean you agree to promotional messages.

We identify mandatory information when requesting it. Without contact information we may be unable to answer you; without necessary application or eligibility information we may be unable to assess or progress an application. Optional information and optional marketing consent are not conditions of making an enquiry.

Please do not include health information, ethnic origin, religious beliefs or other sensitive details in general enquiries or CVs unless requested for a specific need. Before collecting special-category or criminal-offence information, we will explain the purpose, applicable additional legal condition and safeguards in a separate notice.

Cookies, sharing & retention

HOW INFORMATION IS HANDLED

6. Cookies and similar technologies

Cookies and similar technologies can store or access information on your device. Strictly necessary technologies support requested website functions or security. Under this policy, optional analytics, advertising and non-essential embedded-content tracking will be used only after you actively agree.

Where optional technologies are used, we will provide their names, providers, purposes and lifetimes with cookie controls before activation. You can reject optional technologies and revisit your choices through those controls. Browser settings can also delete or block cookies, although some functions may then be unavailable. Continuing to browse is not consent.

7. Who may receive information

We share only information necessary for the relevant purpose with authorised personnel and, where used, providers of hosting, IT support, business email, secure storage, enquiry management and recruitment administration. Service providers acting on our instructions must protect the information under appropriate written contracts.

Relevant information may also go to professional advisers, insurers, banks or payment providers for business administration, and authorities where disclosure is required by law. A proposed business transfer may require limited disclosure to advisers and a prospective successor, subject to appropriate confidentiality and lawful safeguards.

Client campaigns: where we collect customer information for a brand, charity or other client, the campaign notice will identify the controller, recipients, purposes and legal basis before collection. Where we act only as a processor, the client determines the use of that information. This website notice does not authorise sharing applicants or website enquirers with clients for unrelated marketing.

8. International transfers

Some suppliers may store or access information outside the UK. Before any restricted transfer, we will establish a lawful mechanism, such as applicable UK adequacy regulations or approved contractual safeguards, including the UK International Data Transfer Agreement or UK Addendum where appropriate, with the required risk assessment and supplementary protections. Ask our privacy contact for the relevant destinations and a copy or explanation of the applicable safeguards.

9. How long we keep information

We keep information only while needed for its purpose. Enquiries are retained until resolved and for a justified follow-up or dispute period. Recruitment records are kept through the process and for a proportionate period to address challenges; any future-opportunity retention has a separately stated end date and consent.

Contract and financial records follow applicable accounting, tax and claim periods. Security logs follow the period necessary to detect and investigate incidents. Marketing records are reviewed for continuing relevance; suppression records remain only as needed to honour objections. Legal holds may extend retention for specific records. We securely delete or anonymise data when the applicable need ends, with backups removed through their normal protected rotation.

Your rights & contact

CONTROL OVER YOUR PERSONAL INFORMATION

10. Keeping information secure

We use appropriate technical and organisational measures proportionate to the information and risk, including controlled access and confidentiality requirements. We limit access to people who need it for their work and review supplier arrangements. No online transmission or storage method is completely secure. If a breach occurs, we assess it and notify the regulator and affected people where legally required.

11. Your data protection rights

Depending on the circumstances, you can request access to your personal information, correction of inaccurate information, erasure, restriction of processing, and a portable copy of information you supplied where processing is automated and based on consent or contract. You can also withdraw consent.

Your right to object: you may object to processing based on legitimate interests because of your particular situation. We must then stop unless we can demonstrate overriding compelling legitimate grounds or the processing is needed for legal claims. Your right to object to direct marketing is absolute.

Contact admin@unionmarketing.co.uk to exercise a right. We may need proportionate identity verification. We normally respond within one month, without charge. If a permitted extension or exception applies, we will explain it and your options within the applicable deadline.

12. Automated decisions and children

The activities described in this draft do not include decisions made solely by automated processing that produce legal or similarly significant effects, such as automatic rejection of applicants. If such processing is introduced, we will provide the required information and safeguards before it occurs.

Our business website is not directed at children. If you believe a child has provided information unnecessarily, contact us so we can review and remove it where appropriate. Any recruitment of younger applicants requires age-appropriate privacy information and safeguards.

13. Complaints

Please contact us if you are concerned about how information is handled. You can also complain directly to the Information Commissioner's Office (ICO), the UK data protection regulator, without first complaining to us.

ICO: ico.org.uk/make-a-complaint/

Telephone: 0303 123 1113

Address: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Where the EU GDPR applies to particular processing, you may also complain to the competent supervisory authority in the EEA, including where you live or work or where the alleged infringement occurred.

14. Changes to this policy

We will update this policy when our activities or applicable requirements change and make the revised version available on our website. Material changes will be brought to your attention where appropriate. The effective date requested for this version is 1 January 2026; it does not establish when the notice was first published.

Owner review note

INTERNAL ONLY | REMOVE THIS PAGE FROM THE PUBLIC VERSION

Status: a tailored draft, not a certification of compliance. Prepared from the public website reviewed on 16 September 2026. The requested effective date is 1 January 2026; historical adoption or publication has not been verified. Do not describe this draft as a policy actually published on that date unless records support it.

Confirm before publishing

Controller identity: confirm the exact legal person operating as Union Marketing and insert its full legal name in section 1. Confirm the published address, email and phone are current. Add a DPO or representative contact if required. No company number or legal identity has been inferred from the trading name.

Actual processing: verify the enquiry and application routes, fields collected, recruitment sources, reference checks, mandatory eligibility checks, younger applicants, sensitive information and automated tools. Remove activities that do not occur and add any missing ones. Agree a lawful basis for each real purpose.

Cookies: perform a live cookie and tracking audit, including embedded content and third-party scripts. Publish the actual names, providers, purposes and lifetimes. Implement and test consent controls before using optional tracking. Website text alone did not establish the presence or absence of tracking.

Suppliers and transfers: confirm the hosting, email, storage, recruitment and other providers; their processing locations; written processor contracts; and any actual transfer mechanism. Replace conditional transfer wording with the confirmed arrangements. Assess whether EU GDPR obligations also arise.

Retention and operations: adopt justified retention periods and deletion routines for each record type. The draft uses purpose-based criteria because existing periods were not supplied. Verify security controls, rights handling, complaint procedures and any required ICO fee registration.

Campaigns and marketing: confirm the division of controller and processor responsibilities with each client. Provide campaign-specific privacy notices. Confirm marketing channels, consent records and suppression procedures. Do not assume website enquiries or job applications provide marketing permission.

Once verified, remove the draft labels and this internal page, approve the notice and link it prominently from the website and each collection point. Keep an accurate publication and revision record. An effective-date label does not cure earlier non-compliance.

Reference material

Business details: [Union Marketing website](#). Drafting references: ICO guidance on [privacy information](#), [lawful bases](#), [individual rights](#), [international transfers](#) and [cookies](#). Current guidance includes updates after the requested effective date; this draft is not a retrospective legal audit.