Fire Horse26 Privacy Policy

Full policy for review • Draft dated 8 October 2026

This policy explains how Fire Horse26 Ltd collects, uses, shares and protects personal information through our website, consultancy services, commercial subscriptions and Members' Lounge. It also explains your rights and how to contact us.

Review note: Complete the highlighted contact placeholders and check the matters in the final review checklist before publishing. The checklist is for internal review and does not form part of the website policy.

1 Who we are and how to contact us

Fire Horse26 Ltd ("we", "us" or "our") provides commercial consultancy and subscription support, including contract administration, procurement, cost assurance and claims support. We are the data controller for personal information we use to manage our business, website, enquiries, memberships and marketing.

Website: www.firehorse26.co.uk
Privacy contact email: info@firehorse26.co.uk
Postal contact address: 87 Church Street, Crowthorne, Berkshire, RG24 7AW

We handle personal information in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003 (PECR), as amended. Where applicable, we also comply with the EU GDPR.

Where we process personal information solely on a client's instructions, the client is normally the controller and we act as a processor under agreed data processing terms. For that processing, the client's privacy notice also applies. We will help direct rights requests to the appropriate controller.

2 Information we collect

- Contact and business details, such as your name, role, employer, email address, telephone number and correspondence address.
- Enquiry and service records, including emails, WhatsApp messages, meeting notes, advice requests and instructions.
- Membership information, including account registration and authentication data, membership tier, subscription status, renewal dates and support requests.
- Billing and payment records, including invoices, payment amounts, dates, references and relevant bank transaction information.
- Personal information contained in client documents, such as contracts, valuations, payment applications, tender records, labour records, claims and project correspondence.
- Technical and usage data processed through our website, such as IP addresses, browser information, login activity, cookie preferences and use of website or membership resources, depending on the features enabled.
- Marketing preferences, consent records and unsubscribe or objection records. Where tracking is enabled and lawfully permitted, email engagement information may also be collected.

3 Where information comes from

We collect information when you contact us, complete website forms, register for membership, subscribe to updates, use our website or instruct us to provide services. We also receive information from client

organisations and their authorised representatives, professional advisers and project participants where needed for our work.

Where relevant, business contact details may come from publicly available company websites, professional directories, professional networking profiles or referrals. We use this information only where we have an appropriate lawful basis and comply with applicable marketing rules. You can ask us where we obtained your information.

Please share only personal information necessary for the agreed work and ensure you have authority to disclose it. We do not routinely request health information or other special category data, or criminal offence data. If such information is necessary for an engagement, we will first establish the additional legal conditions and safeguards required.

4 Why we use information and our lawful bases

We use the lawful basis appropriate to each purpose. A contract with a company does not automatically provide a contractual lawful basis for processing its employees' personal information.

- Enquiries and quotations: taking steps at your request before entering a contract with you; otherwise our legitimate interest in responding to business enquiries and arranging services.
- Consultancy and membership delivery: performing a contract with you as an individual; for representatives of corporate clients, our legitimate interest in managing the client relationship, providing advice and administering authorised access.
- Invoicing and payments: performing a contract with you where applicable, our legitimate interest in administering corporate client accounts and recovering amounts owed, and legal obligations concerning accounting and tax records.
- Website operation, account security and misuse prevention: our legitimate interest in maintaining reliable and secure services. Consent is used for cookies or similar technologies where required.
- Marketing: consent where required, or legitimate interests where permitted by UK GDPR and PECR, as explained in Section 8.
- Complaints, disputes and legal claims: our legitimate interest in responding to concerns and establishing, exercising or defending legal claims; legal obligations where applicable.

When relying on legitimate interests, we assess whether the processing is necessary and balance those interests against your rights, freedoms and reasonable expectations.

You do not have to provide information for optional marketing. If you do not provide information needed to respond to an enquiry, administer an account, meet a legal requirement or deliver an agreed service, we may be unable to carry out that activity. We will explain any relevant requirement when collecting the information.

5 Members Lounge accounts

Our Wix website provides individual member logins for access to the Members' Lounge and resources. Wix processes registration and authentication information as part of providing the platform. We use account information to manage access, subscription status and support. Keep your login details confidential and notify us promptly of suspected unauthorised access.

6 Payments and client documents

Membership and consultancy payments are administered by invoice and bank transfer. We do not currently take membership payments through the website or request or store payment card details through it. Relevant billing and bank transaction records are used for payment administration and financial record keeping.

Clients send documents by email or secure cloud links. We do not currently offer direct client document uploads through our website. We use Microsoft OneDrive to store, manage and share relevant client and business documents. Access is limited to authorised people who need information to provide services or carry out related business duties.

Please agree an appropriate sharing method with us before sending particularly sensitive personal information or confidential project records. We use appropriate technical and organisational measures, including access controls and account protection, taking account of the nature and risks of the information.

7 Email and WhatsApp communications

We use email and WhatsApp for enquiries, service support, appointments and membership communications. This may involve contact details, message content and attachments. Relevant correspondence is kept where needed to deliver services, record instructions or deal with queries and disputes.

WhatsApp and its associated providers process certain information under their own privacy terms. Please use agreed secure document sharing arrangements for sensitive records rather than sending them through routine WhatsApp messages. Choosing to contact us on WhatsApp does not itself amount to consent to receive marketing.

8 Email marketing

We use Wix Email Marketing to send information about our consultancy services, subscriptions, resources, events and business updates. Marketing is optional and is separate from essential account, invoice and service communications.

For individuals, sole traders and certain partnerships, we obtain consent before sending electronic marketing unless the statutory soft opt-in applies. We use the soft opt-in only where we obtained your contact details during a sale or negotiations for a sale of our services, market our own similar services, and offered a clear opt-out both when collecting your details and in each message.

For corporate business contacts, we may rely on legitimate interests to send relevant business marketing where permitted, after considering the necessity of the processing and its impact on the person concerned. A publicly available email address is not, by itself, consent to marketing.

Your right to stop marketing: You can object to direct marketing at any time or withdraw consent by using the unsubscribe link or contacting our privacy email address. We will stop using your information for direct marketing after an objection. This does not affect essential service communications or the lawfulness of processing before consent was withdrawn.

We may keep a minimal suppression record so we can honour your opt-out and avoid adding you to future campaigns. We do not sell or trade personal information or marketing contact lists.

9 Cookies and similar technologies

Our Wix website uses cookies and similar technologies. Some are necessary for website functions, security, member authentication or remembering your choices. Optional analytics or marketing technologies, where enabled, are used only on an appropriate legal basis, including consent where required.

You can manage optional technologies through the website’s cookie controls and change your choices later. Our cookie information should identify the technologies actually used, their purposes, providers and durations. Browser settings can also restrict cookies, although this may affect website functionality.

10 Who we share information with

We share personal information only where necessary for the stated purposes and where a lawful basis applies. Recipients may include:

- Wix, for website hosting, member accounts, website forms and email marketing.
- Microsoft, for OneDrive storage and sharing, and any Microsoft business services we actually use.
- WhatsApp and associated service providers, for communications through that channel.
- Email, IT support and security providers used to operate our business systems.
- Banks, accountants, insurers, legal advisers and authorised consultants where necessary for payments, business administration, service delivery or legal matters.
- Client representatives and project participants where information must be shared to carry out an authorised engagement.
- Courts, regulators, public authorities or other recipients where disclosure is legally required or necessary to establish, exercise or defend legal rights.

Where providers act as processors, we put appropriate contractual arrangements in place. Some providers or advisers may act as independent controllers for their own activities. Their privacy notices explain that processing. If our business is reorganised or transferred, necessary information may be shared with relevant parties subject to appropriate safeguards and notice where required.

11 International transfers

Some technology providers may store or access personal information outside the UK. Where a restricted transfer takes place, we use an applicable UK adequacy regulation or appropriate safeguards, such as the UK International Data Transfer Agreement or UK Addendum to standard contractual clauses, together with any required assessment and supplementary measures.

You can contact us for information about the safeguards relevant to your data and how to obtain a copy, subject to appropriate redactions. We do not assume that all information remains in the UK simply because a service is cloud based.

12 How long we keep information

We retain personal information only for as long as necessary for the purpose for which it was collected. We determine the period by considering the nature of the record, whether an enquiry or membership remains active, what is needed to complete the engagement, statutory record keeping requirements, and any relevant complaints, disputes or legal claims.

- Enquiries: until dealt with and for any further period needed for agreed follow-up or a relevant complaint or dispute.
- Membership and service records: while needed to administer the relationship and thereafter only where necessary for outstanding obligations, relevant legal claims or applicable record keeping requirements.
- Financial records: for the applicable accounting and tax retention period, or longer only where another lawful requirement applies.
- Marketing records: while the marketing purpose and lawful basis remain valid; minimal opt-out records are retained as needed to respect your choice.
- Technical logs and cookie data: for periods appropriate to their operational purpose and the settings and durations disclosed in our cookie information.

We review records and securely delete, destroy or anonymise information when no longer needed. Deleted information may remain in restricted backups until the normal backup cycle expires. Where we act as a processor, return and deletion are governed by the agreed client instructions and applicable legal requirements.

13 Your data protection rights

Depending on the processing and applicable law, you may have rights to access your personal information, correct inaccurate information, request erasure, restrict processing, receive certain information in a portable format and withdraw consent. These rights are subject to applicable conditions and exceptions.

Right to object: You can object to processing based on legitimate interests on grounds relating to your situation. You also have an absolute right to object to processing for direct marketing, including related profiling.

Contact us using the privacy contact details in Section 1 to exercise your rights. We may need proportionate information to verify your identity. We normally respond within one month, subject to lawful extensions or other adjustments allowed by the applicable rules. Requests are normally free of charge, subject to statutory exceptions.

14 Complaints

Please contact us if you have a concern about our use of personal information so we can investigate and respond. You can also complain to the Information Commissioner's Office (ICO), the UK data protection regulator, without having to complain to us first.

ICO website: https://ico.org.uk/make-a-complaint/
Telephone: 0303 123 1113
Postal address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

15 Children and automated decisions

Our website and commercial membership services are intended for business users and are not directed at children. If we become aware that a child has provided personal information through these services, we will assess what action is appropriate, including deletion where necessary.

We do not intend to make decisions producing legal or similarly significant effects about you solely by automated processing. If we introduce such processing, we will explain it and provide the information and safeguards required by law before using it.

16 Changes to this policy

We may update this policy to reflect changes to our services, providers or legal requirements. The current version and update date will appear on our website. We will bring material changes to your attention where appropriate or required.

Last updated: 08 October 2026

Internal review checklist

Remove this section and the opening review note before publishing the website policy.

- Complete the website, privacy email and postal contact details. Confirm the mailbox is monitored and set the publication date.
- Confirm the OneDrive account type. Use a suitable business arrangement and check processing terms, access permissions, authentication and international transfer arrangements. The draft does not assume OneDrive for Business is already in place.
- Check Wix cookie controls, enabled analytics, email tracking and member data settings. Provide accurate cookie details and ensure optional tracking is controlled as required.
- Verify actual service provider contracts and transfer safeguards; check that security and deletion practices match the policy. Maintain an internal retention schedule with concrete periods for each record type.
- Record marketing consent or the applicable alternative basis and opt-out evidence. Assess the ICO data protection fee requirement and use processor agreements where required for client work.

Drafting references checked on 8 October 2026: ICO privacy notice checklist; ICO guidance on writing a privacy notice; ICO business to business marketing guidance. Guidance should be checked again if publication is delayed or business practices change.