Privacy Policy

225 Fire Solutions Ltd | Website and professional services

Last updated: 25 September 2026 **Version:** 2.1

1. Who we are and how to contact us

225 Fire Solutions Ltd is responsible for the personal information covered by this policy where we decide why and how it is used. In data protection law, this makes us the **data controller**.

Company number: 16853193
Correspondence address: Office 5, The Exeter Business Hub, Queensgate House, 48 Queen St, Exeter, EX4 3SR
Email: 225firesolutions@gmail.com
Website: www.225firesolutions.com

Please address privacy enquiries to the Directors. You can use the email or postal address above to ask questions, exercise your rights or raise a complaint.

2. What this policy covers

This policy explains how we handle personal information relating to website visitors, enquiries, clients, client representatives, suppliers and people whose information is included in our fire safety work. It covers fire risk assessments, inspections, independent reviews, consultancy, training and digital product enquiries or purchases, where provided.

We apply the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003 (PECR), as amended, including relevant changes made by the Data (Use and Access) Act 2025.

If we act solely on a client's documented instructions as a data processor for a particular activity, the client's privacy information and our processing agreement also apply. We explain any additional use of personal information when needed.

3. Personal information we collect

• **Contact and business details:** names, email addresses, contact numbers supplied to us, postal or site addresses, employer, job title and relevant site contact details.

• **Enquiries and transactions:** correspondence, quotations, booking details, contracts, invoices, payment status, purchase records and complaints.

• **Assessment records:** relevant inspection notes, reports, photographs, plans, training or evacuation records and information about building occupants where needed for the agreed service.

• **Website information:** IP address, browser and device information, pages visited, interactions, cookie identifiers and privacy preferences, depending on the technologies in use and your choices.

We seek only information relevant to the task. Please avoid sending unnecessary personal, medical or confidential information through general enquiry forms.

How we use information

4. Where information comes from

We receive information directly from you through forms, email, correspondence, purchases and site visits. We may also receive relevant information from the client who commissions our work, an employer, landlord, managing agent, building owner, responsible person or an authorised representative.

For business enquiries or verification, sources may include company websites, Companies House and business information you make public on social media. Technical website information may come from our website and service providers. Where information comes from another source, we provide privacy information as required by law.

5. Purposes and lawful bases

We use a lawful basis appropriate to each activity. Where we rely on legitimate interests, we consider whether the use is necessary and whether your interests and rights override it.

Purpose	Lawful basis and explanation
Responding to enquiries, preparing quotations and delivering services or downloads	Contract: taking requested steps before a contract with you, or performing that contract. For business contacts and other relevant people who are not personally contracting with us, legitimate interests in arranging and delivering professional services.
Assessments, inspections, reports, quality checks and supporting records	Contract where the individual is our client; otherwise legitimate interests in assessing fire safety, producing reliable advice, maintaining evidence of our work and supporting clients' safety arrangements.
Invoices, accounts and administration	Contract for payment administration; legal obligation where tax or accounting law requires records; legitimate interests in managing accounts and recovering sums owed.
Complaints, insurance and legal matters	Legitimate interests in investigating concerns, maintaining professional accountability and establishing or defending claims; legal obligation where disclosure or other action is legally required.
Website operation, security and improvement	Legitimate interests in providing a secure, usable website and preventing misuse. Consent for cookies or similar technologies where PECR requires it.
Marketing and publicity	Consent where required; otherwise legitimate interests in promoting relevant services, subject to PECR and your right to object. See section 11.

6. Information needed to provide a service

Providing information for an enquiry is generally voluntary. We may need contact, site, access, invoicing or relevant safety information to quote accurately or complete a service. If necessary information is withheld, we may be unable to proceed or may need to limit our assessment. We explain this where relevant. Marketing consent is optional.

Sensitive information and sharing

7. Occupant information and photographs

Fire safety work may reveal information about an identifiable person's disability, health or need for evacuation assistance. We aim to record practical safety needs without collecting unnecessary diagnoses or medical histories. Where possible, reports use anonymous or general descriptions.

Identifiable health information requires an Article 6 lawful basis **and** an Article 9 condition. Before collecting it for a specific service, we identify the applicable condition and provide any additional privacy information needed. This may be explicit consent where appropriate, or another condition whose requirements are met, such as necessity for legal claims. A client's instruction or a general reference to fire safety does not, by itself, supply this condition.

Please contact us before sending identifiable health information or detailed records about children or vulnerable people. We limit access and sharing to what is necessary for the particular purpose.

Site photographs are used to document relevant conditions and support our findings. We aim to avoid unnecessary images of people, personal documents or private possessions, and to crop or obscure identifying details where appropriate. Publishing identifiable people or confidential client material for publicity requires a separate lawful basis and any necessary permissions.

8. Who receives information

We share information only where necessary for the purpose and where there is a lawful basis. Recipients may include:

• Directors, assessors, authorised staff and specialist consultants involved in delivering or checking the work.

• The commissioning client and authorised building representatives, such as the responsible person or managing agent, where relevant to the report or agreed service.

• Providers of website hosting and forms, email, cloud storage, report management, accounting and payment services. These include Wix for the website and RiskBase, where we store fire risk assessments and other assessment data.

• Accountants, legal advisers, insurers and professional auditors where required for administration, quality assurance, complaints or claims.

• Fire and rescue services, local authorities, courts, regulators or other public bodies where disclosure is required by law or otherwise necessary and lawful.

Service providers acting on our behalf must process information under appropriate contractual terms. Some recipients, such as regulators or payment providers, may act as independent controllers and provide their own privacy notices. We do not sell personal information.

9. International transfers and security

Website, email and cloud service providers may store information, or permit support access, outside the UK. Where this is a restricted transfer, we use a permitted transfer mechanism: applicable UK adequacy regulations or appropriate safeguards, such as the UK International Data Transfer Agreement or UK Addendum, with the required assessment. You can contact us for details of relevant destinations and a copy or explanation of the safeguards, subject to necessary redactions.

We use appropriate technical and organisational measures to protect information and restrict access to those who need it. No system is entirely risk-free. Suspected loss, misuse or unauthorised access should be reported using our contact details. We assess incidents and notify affected individuals and the ICO where legally required.

Retention, marketing and cookies

10. How long we keep information

We keep personal information only for as long as reasonably necessary for its purpose. Where a fixed period cannot be stated for every record, we determine retention using the following criteria:

• **Enquiries and quotations:** the time needed to answer the enquiry, complete any agreed follow-up and resolve related questions. Unsuccessful enquiries are reviewed for deletion when no longer needed.

• **Assessment reports, site notes and photographs:** the agreed service, the need to evidence our findings and advice, contractual commitments, applicable claim periods and relevant insurance or regulatory requirements. We limit the personal detail retained and review continued need.

• **Accounts and transaction records:** applicable tax and accounting retention requirements, together with any unresolved payment or audit matters.

• **Complaints and claims:** the time needed to investigate, resolve and demonstrate the handling of the matter, plus any necessary legal or insurance retention.

• **Marketing preferences:** while relevant marketing continues, with a minimal suppression record retained where necessary to honour an opt-out. Cookie and website data retention depends on the specific technology and its stated duration.

A relevant legal hold, investigation or dispute may require longer retention. When information is no longer required, we securely delete or anonymise it. Residual backup copies are restricted and expire through the applicable backup cycle. You can ask us about the retention period or criteria for a particular record; deletion rights are subject to lawful retention needs.

11. Marketing communications

Service messages, such as booking confirmations and report delivery, are sent to administer your enquiry or contract. Where we send marketing by email or similar electronic messages to individuals, sole traders or relevant partnerships, we obtain consent unless all conditions of the customer soft opt-in apply.

The soft opt-in applies only where we obtained your details directly during a sale or genuine sales negotiation, market our own similar services or products, and offered a clear opt-out both when collecting the details and in each message. We may send relevant business marketing to corporate subscribers where PECR allows this, using legitimate interests for personal contact details after considering your rights.

You can stop direct marketing at any time using the unsubscribe option or by contacting us. We respect objections and do not require you to give a reason.

12. Cookies and similar technologies

Our website may use cookies or similar technologies for essential functions, preferences, audience measurement and advertising. Their use depends on the features enabled and your choices. Strictly necessary technologies may operate without consent. Advertising and other non-exempt technologies require prior consent.

Analytics are not automatically exempt. We rely on a statistical or other PECR exception only where all its conditions are met, including clear information and an easy way to object where required. Otherwise we seek consent. Consent can be withdrawn without affecting the lawfulness of earlier use.

The website’s cookie information and controls should be read alongside this policy for details of the technologies actually in use, their providers, purposes and durations. You can also manage stored cookies in your browser; blocking essential cookies may affect site functions. Contact us if you need help with your choices.

Your rights and enquiries

13. Your data protection rights

Depending on the circumstances and the lawful basis used, you can:

• Ask for access to your personal information and a copy of it.

• Ask us to correct inaccurate information or complete information that is incomplete.

• Ask us to erase information or restrict its use where the relevant conditions are met.

• Object to processing based on legitimate interests. We will consider your situation and stop unless we have grounds permitted by law to continue.

• Object to direct marketing at any time. This right is absolute for that purpose, including related profiling.

• Request portability of information you provided where processing is automated and based on consent or a contract, and the right applies.

• Withdraw consent at any time where we rely on it. Withdrawal does not affect processing already lawfully carried out.

To make a request, contact **225firesolutions@gmail.com** or write to the address in section 1. We may request proportionate information to verify identity or clarify the request. Requests are normally free, and we normally respond within one month. Where the law permits an extension, pause, fee or refusal, we explain the reason and any applicable revised timescale.

Rights are not unlimited. For example, we may need to keep certain records for legal obligations or claims, and must protect other people's information when providing access.

14. Automated decisions

We do not use solely automated decision-making to make decisions about you that have legal or similarly significant effects. Professional assessment findings and advice involve human judgement. Website analytics or advertising tools, where enabled, may analyse interactions or interests as explained in the relevant cookie information.

15. Questions and complaints

If you are concerned about our use of your information, please contact the Directors using the details in section 1 and describe the concern. We will acknowledge a data protection complaint within 30 days, investigate appropriately, keep you informed and communicate the outcome without undue delay. This complaints process does not replace the separate timescales for rights requests.

You also have the right to complain to the Information Commissioner's Office (ICO). You do not need our permission to do so.

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

16. External websites and policy updates

External websites and social media platforms have their own privacy arrangements. This policy explains our handling of information and does not govern those independent services.

We review this policy when our services, practices or legal requirements change. The latest version will be made available on our website with an updated date. Where a change materially affects how we use information, we will provide appropriate notice and obtain fresh consent where required. Continuing to use our website does not, by itself, constitute consent.