Security & responsible automation

Practical protection, clear responsibility

How the website is protected and the principles used when WeekFound builds and supports automation.

Source last updated: 21 September 2026. Project-specific controls are agreed according to the systems, information and risk involved.

Our approach

WeekFound uses proportionate, practical safeguards and designs systems so their operation remains understandable. No website or automation can be guaranteed completely secure. We review the controls needed for the information, access and consequences involved rather than applying the same design to every project.

Website protection

The public website is delivered over HTTPS and uses Cloudflare protection to help identify and reduce malicious or automated traffic. Browser security headers restrict framing, content sources, referrer information and access to device features. The underlying hosted address and the shorter domain redirect to one canonical public address, including API routes, so an unattended duplicate is not left operating separately.

Authentication and request limits

The client Workspace uses passwordless sign-in links rather than stored passwords. Each link contains a cryptographically random token, expires after 15 minutes and can be used only once. Login requests receive the same public response whether or not an account exists, and sign-in, enquiry and AI-assessment routes are rate limited by privacy-preserving hashed identifiers to reduce automated abuse. Sessions and login tokens are stored as hashes, and the session cookie is HTTP-only, secure over HTTPS and limited to same-site use.

Access, secrets and data boundaries

Service credentials are kept in the hosted server environment rather than placed in public website code. Connections to the private customer-management system use authenticated requests. Website databases and private files are accessed only through server routes; Workspace queries are restricted to the signed-in customer's workspace. For client work, access should belong to the client wherever practical and receive only the permissions needed for the agreed workflow.

Data minimisation

The enquiry form asks for only the details needed to understand and answer a request. Visitors are told not to submit passwords or unnecessary sensitive personal information. Project discovery identifies what data is genuinely needed, where it will be stored, who can access it and when it should be removed.

AI-assisted processing

Where an optional assessment uses an AI provider, WeekFound withholds the visitor's name and email address from the analysis request and configures the request not to be stored by that provider. AI output is treated as a preliminary draft, not proof of feasibility, security or compliance.

Testing and human approval

Client automations are tested with representative examples, expected exceptions and agreed acceptance criteria before launch. Sensitive communications, financial actions and decisions affecting people retain meaningful human approval. Material changes return to review and testing before broader use.

Monitoring and recovery

Important production workflows should have a named owner, visible failure information, a client-operated retry or restart control where appropriate, and an agreed manual fallback that is tested before launch. Website and email-delivery errors are recorded by the relevant services, and the contact page provides hello@weekfound.co.uk as an alternative when online sending is unavailable. Project-specific monitoring, backup and response commitments are recorded in the project or care-plan documents.

Security incidents and personal data breaches

WeekFound maintains an incident process to contain a suspected breach, preserve useful evidence, understand which systems and information are affected, recover safely and record the decisions made. Where personal information is involved, we assess the likely risk to people and meet any applicable notification duties, including notifying the Information Commissioner's Office within 72 hours where UK data-protection law requires it and informing affected people without undue delay where the risk is high. Contractual responsibilities and client communications are handled alongside, not instead of, those legal duties.

Suppliers and client control

Third-party services are selected for a defined purpose and are documented where they process client or visitor information. Their availability and security remain partly outside WeekFound's control, so projects use sensible fallbacks and avoid unnecessary lock-in. Clients receive documentation and an understandable route to continue or recover the process.

Report a security concern

Email hello@weekfound.co.uk with the subject 'Security concern' and include the affected page or service, what you observed and how we can contact you. Please do not access other people's information, disrupt the service or include live passwords, secret keys or unnecessary personal data in your report. We will acknowledge a credible report and investigate it proportionately.