

SafePass247 Privacy Policy

1. ABOUT THIS POLICY

- 1.1 This Privacy Policy explains how **SafePass247 Ltd (SafePass247, we, us, our)** collects and uses personal information when you visit safepass247.co.uk, use the SafePass247 platform or its applications (the **Platform**), or otherwise deal with us.
- 1.2 **SafePass247 Ltd**, is a company registered in England and Wales under company number 17434264 whose registered office is at 42a Walnut Road, Chelston, Torquay, United Kingdom, TQ2 6HS.
- 1.3 If you have any questions about this policy or how we use your information, please contact us at accounts@safepass247.co.uk or write to us at our registered office. We may update this policy from time to time. The latest version will always be on our website, and we will tell Platform users about significant changes.

2. OUR ROLE — CONTROLLER OR PROCESSOR

- 2.1 The Platform is used by businesses (our **Customers**) to manage Risk Assessments and Method Statements (**RAMS**) and related health and safety documents for their projects. Customers invite their own staff, advisors, and contractors and subcontractors to use the Platform.
- 2.2 **Where we decide how and why your information is used, we are the controller.** This covers information we use to set up and manage accounts, run and secure the Platform, deal with enquiries and billing, improve our services and market to business contacts.
- 2.3 **Where we handle information on behalf of a Customer, the Customer is the controller and we are its processor.** This covers the documents, RAMS, comments, approvals, training and competence records and other project content that Customers and their contractors upload or create on the Platform. In those cases, we only use the information on the Customer's instructions and under a contract with it, and the Customer's own privacy notice will explain how it uses your information. If you want to exercise your rights over that information, please contact the relevant Customer (for example, the principal contractor that invited you to the project). If you contact us, we will pass your request on.

3. INFORMATION WE COLLECT

- 3.1 Depending on how you interact with us, we may collect the following:

Category	Examples
Identity and contact information	Name, job title, employer, business email address, telephone number.
Account information	Username, password (stored in encrypted form), multi-factor authentication details, role and permissions, projects you are linked to, account preferences.
Activity and audit information	Documents you upload, review or sign off; comments; actions taken; and the name, role, organisation, date and time recorded against each review or signature (the Audit Trail).

Category	Examples
Project content	Information within RAMS and related documents, which may include names of operatives and supervisors, training and qualification details (for example CSCS or CPCSC card numbers and expiry dates), site induction and attendance records, and emergency contacts.
Technical information	IP address, browser and device type, operating system, log-in times, pages viewed, error logs, and information collected through cookies and similar technologies.
Billing information	Billing contact details, purchase order references, invoices and payment records (card payments are processed by our payment provider and we do not store full card details).
Communications	Emails, support requests, feedback, survey responses and records of calls or meetings with us.
Marketing information	Your marketing preferences, and whether you have opened or clicked on our emails.

- 3.2 **Sensitive information.** The Platform is not designed to hold special category data (such as health information) or criminal offence data. Occasionally RAMS may contain limited health information, for example relating to health surveillance or fitness for work. Customers and contractors are asked to include such information only where strictly necessary and where they have a lawful basis to do so. Where this happens, we handle it as processor on the Customer's behalf and protect it accordingly.

4. WHERE WE GET YOUR INFORMATION

- 4.1 We collect information directly from you when you register, use the Platform, contact us or attend a demonstration or event.
- 4.2 We receive information from your employer or from the Customer that invited you, for example when you are set up as a user or named in an uploaded document. We collect technical information automatically when you use our website or the Platform.
- 4.3 We may obtain business contact information from publicly available sources such as Companies House and professional networking sites, and from referral partners.

5. HOW AND WHY WE USE YOUR INFORMATION

- 5.1 Where we act as controller, we use your information for the following purposes and on the following legal basis under the UK GDPR:

Purpose	Examples	Legal basis
Providing the Platform and managing accounts	Creating and administering user accounts, authenticating users,	Performance of our contract with the Customer, and our legitimate interest in

Purpose	Examples	Legal basis
	routing documents, sending service notifications.	providing the service the Customer has requested for its users. Where you are the Customer (for example a sole trader), performance of our contract with you.
Maintaining the Audit Trail	Recording who reviewed or signed off a document and when.	Our legitimate interest, and that of Customers, in maintaining reliable records of health and safety decisions; and legal claims.
Security and fraud prevention	Monitoring access, detecting misuse, investigating incidents.	Our legitimate interest in keeping the Platform and its data secure; and, where applicable, legal obligation.
Support and communications	Responding to enquiries and support requests.	Our legitimate interest in supporting our users; and performance of contract.
Billing and administration	Invoicing, payment collection, record-keeping.	Performance of contract; legal obligation (tax and accounting).
Improving the Platform	Analysing how features are used, testing and developing new features, using anonymised or aggregated information.	Our legitimate interest in developing and improving our services.
Marketing	Sending news and offers about SafePass247 to business contacts.	Our legitimate interest in promoting our business, subject to your right to opt out at any time. Where the law requires consent (for example for some electronic marketing to individuals), we will ask for it.
Legal and regulatory	Complying with law, responding to requests from regulators, courts and law enforcement,	Legal obligation; our legitimate interest in protecting our rights.

Purpose	Examples	Legal basis
	establishing or defending legal claims.	

- 5.2 Where we rely on legitimate interests, we have considered whether those interests are outweighed by your rights and freedoms. You can ask us for more information about this balancing exercise. If you do not provide information we need, for example to create your account, you may not be able to use the Platform.

6. AUTOMATED REVIEW AND ARTIFICIAL INTELLIGENCE

- 6.1 The Platform uses automated tools, which may include artificial intelligence, to screen RAMS against a set of questions and to highlight possible gaps for a person to review. This analysis relates to documents, not to individuals.
- 6.2 We do not make any decision about you, which has legal or similarly significant effects on you, based solely on automated processing. Decisions about whether to accept RAMS are made by people using the Platform.
- 6.3 Where we use a third-party artificial intelligence provider to deliver these tools, it acts as our sub-processor, does not use your information to train its own models, and is subject to the safeguards described in section 8.

7. WHO WE SHARE YOUR INFORMATION WITH

- 7.1 We share information only where necessary, with:
- (a) **the Customer and other project participants** — information you upload or actions you take on a project will be visible to the Customer that controls the project, and to other users that Customer permits to see it;
 - (b) **our service providers**, who act on our instructions, including Supabase and our IT and security contractors;
 - (c) **our professional advisers**, including lawyers, accountants and insurers;
 - (d) **regulators, courts and law enforcement bodies**, including the Health and Safety Executive or the police, where we are required or permitted by law to do so; and
 - (e) **a buyer or investor**, if we sell, merge or restructure our business, subject to appropriate confidentiality protections.
- 7.2 We do not sell personal information.

8. INTERNATIONAL TRANSFERS

- 8.1 We host the Platform and project content in the United Kingdom.
- 8.2 Some of our service providers may process information outside the UK. Where this happens, we make sure the transfer is protected, either because the country benefits from UK adequacy regulations (as the EEA does) or because we use approved safeguards such as the ICO's International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses. You can ask us for more information about these safeguards.

9. HOW LONG WE KEEP YOUR INFORMATION

- 9.1 We keep personal information only for as long as we need it for the purposes described in this policy. In general:

Information	Retention period
Account information	For as long as your account is active, and for 12 months after it is closed.
Project content and Audit Trail (as processor)	As directed by the Customer during its subscription, and deleted within 30 days after the subscription ends, unless the Customer asks us to export it or the law requires us to keep it.
Billing and contract records	Six years from the end of the financial year to which they relate.
Support and communications	3 years from the date of the last contact.
Technical and security logs	12 months, unless needed to investigate an incident.
Marketing information	Until you unsubscribe, or after 2 years without engagement; we keep a suppression record so that we do not contact you again.

9.2 Customers are responsible for deciding how long to keep RAMS and related records, which may be required for health and safety, contractual or insurance reasons long after a project ends.

9.3 We may keep anonymised information, which no longer identifies anyone, indefinitely.

10. HOW WE PROTECT YOUR INFORMATION

We use appropriate technical and organisational measures to protect personal information, including encryption in transit and at rest, UK hosting in secure data centres, role-based access controls, access logging, regular back-ups and security testing, and staff confidentiality obligations. No system is completely secure, so please keep your login details safe and tell us immediately if you think your account has been compromised.

11. YOUR RIGHTS

11.1 Under data protection law you have the right to:

- (a) be informed about how your information is used (which is the purpose of this policy);
- (b) access the personal information we hold about you;
- (c) have inaccurate information corrected and incomplete information completed;
- (d) have your information erased in certain circumstances;
- (e) restrict how we use your information in certain circumstances;
- (f) object to our use of your information where we rely on legitimate interests, and to object at any time to direct marketing;

- (g) receive your information in a portable format, where we rely on contract or consent and process it by automated means;
- (h) withdraw consent at any time, where we rely on consent; and
- (i) not be subject to decisions based solely on automated processing which have legal or similarly significant effects on you, save where permitted by law and subject to safeguards.

11.2 Some of these rights are subject to conditions and exemptions. For example, we may not be able to delete Audit Trail records that a Customer needs to keep, or that we need for legal claims.

11.3 To exercise any of these rights, contact us at accounts@safepass247.co.uk. We may need to verify your identity. We will respond within one month, which may be extended by up to two further months for complex requests. We do not usually charge a fee.

11.4 Where we process your information as a processor for a Customer (see section 2.3), we will pass your request to the Customer and help it to respond.

11.5 You can unsubscribe from our marketing emails at any time using the link in each email.

12. COOKIES

Our website and Platform use cookies and similar technologies. Some are strictly necessary for the Platform to work, for example to keep you logged in securely. We use other cookies, such as analytics cookies, only in accordance with the law and your choices. For more information, please see our Cookie Notice at safepass247.co.uk/cookies.

13. CHILDREN

Our website and Platform are intended for business use and are not directed at children. Platform users must be at least 18.

14. LINKS TO OTHER WEBSITES

Our website may contain links to other websites, including those of regulators and guidance bodies. We are not responsible for their privacy practices.

15. COMPLAINTS

15.1 If you are unhappy with how we have handled your information, please contact us first at accounts@safepass247.co.uk so that we can try to put things right. We will acknowledge your complaint and investigate it without undue delay and let you know the outcome.

15.2 You also have the right to complain to the Information Commissioner's Office (ICO), the UK regulator for data protection: www.ico.org.uk, telephone 0303 123 1113.

Version 1 - last updated 17 September 2026.