PRIVACY POLICY

Last Updated: 14 November 2025

Staff Secure Ltd Privacy Policy (UK GDPR Compliant)

Introduction & Scope

This Privacy Policy explains how Staff Secure Ltd ("we", "us", "our") collects, uses, shares, and protects personal information when users access or interact with our HR management platform at staffsecure.ai. We are fully committed to complying with the UK General Data Protection Regulation ("UK GDPR"), the Data Protection Act 2018, and all applicable UK data-protection laws. By creating an account, uploading a CV, submitting job requirements, communicating through the platform, or subscribing to our HR service packages, you acknowledge and agree to the practices described in this Privacy Policy.

- **About Us**

  Staff Secure Ltd is the Data Controller responsible for determining the purposes and methods of processing your personal data. Our registered business address is 124–128 City Road, London, EC1V 2NX, United Kingdom. Staff Secure Ltd operates a digital HR management system that enables employers to post staffing requirements, receive candidate CVs, access placement updates, communicate through chat tools, and manage subscription services, all through a secure online platform. Candidates may create profiles, upload CVs, review job opportunities, communicate with employers, and track their placement progress

- **Who This Policy Applies To**

  This Privacy Policy applies to:

  • Employers who subscribe to our 12-month HR management packages.

  • Candidates who register on the platform and apply for job opportunities.

  • Website visitors who browse, interact, or submit information through staffsecure.ai.

  • Any individual contacting us for support, enquiries, or general communication.

- **What Personal Data We Collect**

  We collect a range of personal and professional data depending on how you use the platform. This includes information provided directly by users as well as data collected automatically through system logs and cookies. We only collect information necessary to provide our services, maintain platform security, process payments, fulfil contractual obligations, or comply with legal requirements. Data categories include identity information, contact details, subscription records, job-related data, uploaded documents, communication logs, and technical usage data.

Employer Data We Collect

When employers create an account or subscribe to one of our HR packages, we collect personal and business information required to manage their subscription and deliver platform services. This includes the employer's full name, company name, business sector, email address, telephone number, profile settings, and user login credentials. We also collect subscription and billing information such as chosen package, instalment plan, payment history, renewal dates, trial period activation, and invoice records. Payment card details are **not stored** by Staff Secure Ltd; instead, they are processed securely through trusted third-party payment providers such as Stripe or PayPal.

Employers also generate usage data during their interaction with the platform. This includes job requirements submitted, CVs viewed, messages exchanged through the live-chat system, placement progress, and dashboard activity logs. We also track notifications, subscription alerts, account modifications, and system interactions. This data allows us to operate your account, deliver HR services, manage your subscription, verify platform activity, and comply with our contractual and legal obligations.

- **Candidate Data We Collect**

  Candidates who create profiles or apply for jobs provide personal, professional, and employment-related data necessary for HR matching and placement support. This includes full name, email address, location, date of birth, skills, qualifications, years of experience, roles of interest, and any additional information added to their professional profile. Candidates may also upload CVs or documents containing sensitive employment information such as work history, education, certifications, references, and contact details. CVs may also include photographs and other identifiers submitted voluntarily.

We collect candidate activity data including job applications, application status updates, CV dispatch details, employer views, chat messages with employers, placement outcomes, and internal system notifications. All candidate data is processed to facilitate introductions between employers and candidates, support job-matching decisions, and manage placement workflows on the platform.

Technical and Automatically Collected Data

When users access or interact with our platform, certain technical information is collected automatically to maintain security, enhance user experience, and support system analytics. This includes IP address, browser type, device type, operating system, access times, authentication tokens, session identifiers, and error diagnostics. We also track page navigation, feature interaction, login attempts, and usage patterns to help us optimise the platform's performance and detect fraudulent or unauthorised activity. This information is gathered through cookies, secure session technology, and automated logging tools operating within our system.

We use cookies to ensure the platform functions correctly, to enable secure login sessions, and to understand how users navigate the website. Cookies also support preference settings, saved filters, dashboard configurations, and analytics required to improve performance. Certain non-essential cookies or tracking tools may require user consent under UK law; these will be presented via a cookie banner when applicable. Users may adjust cookie settings at any time through their browser or via a cookie preferences panel if made available.

- **How We Use Personal Data**
  Staff Secure Ltd processes personal data for several clearly defined purposes. The primary purpose is to deliver HR management services, including creating user accounts, managing subscriptions, presenting job opportunities, forwarding CVs to employers, and facilitating communication between employers and candidates. We use identity, contact, and account information to verify users, maintain secure access, and provide tailored platform features. We process billing information to manage subscriptions, generate invoices, and handle renewals in accordance with the customer's chosen service package.

Candidate data is processed to support job matching, placement decisions, and communication with employers. CVs and professional information are shared only with

employers who require candidates for open roles. Technical and analytics data is used to maintain platform functionality, enhance security protections, diagnose technical issues, and support operational improvement. We may also process data to comply with legal obligations, resolve disputes, prevent fraud, and enforce our Terms & Conditions.

Legal Bases for Processing Personal Data

Under the UK GDPR, Staff Secure Ltd must rely on one or more lawful bases to process personal data. We primarily process data under **Contract Performance**, as employers and candidates require our services to submit job requirements, apply for roles, review CVs, and manage subscriptions. Where data is processed to improve platform functionality, maintain security, or support analytics, we rely on **Legitimate Interests**, ensuring such processing is necessary, proportionate, and does not override user rights. For certain activities—such as storing optional profile data, using non-essential cookies, or sharing candidate CVs with employers—we rely on **Consent**, which can be withdrawn at any time.

We may process personal data under **Legal Obligation** where required to comply with UK tax, accounting, fraud prevention, and regulatory requirements. If exceptionally sensitive employment information is submitted within CVs or profiles, such data is processed strictly for HR matching and with the clear understanding that it has been voluntarily provided by the candidate.

How Candidate CV Data Is Shared

A core function of our platform is to enable the secure forwarding of candidate CVs and professional profiles to employers who request staffing support. When a candidate uploads a CV or applies for a job, they provide explicit consent for Staff Secure Ltd to share this information with relevant employers for recruitment and placement purposes. Employers who receive CVs must use them solely for evaluating suitability for their staffing needs and must comply with UK data-protection law. We track CV dispatch activity, employer views, and updates to ensure transparency and maintain an auditable record of how candidate data is used.

We do not permit employers to share candidate CVs outside their own organisation or store CVs longer than necessary for recruitment purposes. Candidates may request the removal of their CV from our system at any time, although this will not affect any processing already performed lawfully prior to the request. CV forwarding is central to our HR service model, and by choosing to upload a CV, candidates acknowledge and agree to this controlled method of data sharing.

Sharing Personal Data with Third Parties

We may share personal data with trusted third-party service providers who support the operation of our platform and the delivery of our HR management services. These providers assist with secure data hosting, cloud storage, email delivery, analytics, payment processing, customer support, and technical infrastructure. All such third parties are contractually bound to protect personal data, act only on our instructions, and maintain strict confidentiality in accordance with the UK GDPR. Examples include cloud hosting partners, email service platforms, analytics tools, and payment processors such as Stripe or PayPal. We ensure that third-party access is limited, controlled, and used only when necessary to fulfil core service functions.

We may also share limited information with regulatory authorities, law enforcement, or professional advisers when legally required. This may include responding to court orders, complying with tax and accounting obligations, or addressing suspected fraudulent or unlawful activities on the platform. Staff Secure Ltd does **not** sell personal data to any third parties, nor do we permit unauthorised reuse or commercial exploitation of user information for marketing purposes without explicit consent. Employers receiving candidate CVs are prohibited from forwarding data externally unless required for legitimate internal hiring decisions within their organisation.

- **International Transfers of Data**

  Some of our service providers may store or process data outside the United Kingdom. In such cases, Staff Secure Ltd ensures that adequate safeguards are implemented to comply with UK GDPR standards. These safeguards may include the use of countries deemed to offer adequate protection under UK law, the implementation of International Data Transfer Agreements, or the adoption of Standard Contractual Clauses approved by the Information Commissioner's Office (ICO). We require all overseas partners to apply strong security measures and ensure the lawful handling of data transferred internationally. Users may contact us at any

time for more information about the specific safeguards applied to international transfers.

Staff Secure Ltd remains fully responsible for all data transferred to or processed by third parties and ensures that such transfers occur only when necessary and compliant with applicable legal requirements. We continuously monitor our suppliers to verify ongoing compliance with these standards.

Data Security Measures

Staff Secure Ltd implements strong technical and organisational measures to safeguard personal data against unauthorised access, misuse, loss, alteration, and disclosure. Our platform utilises secure, encrypted cloud hosting environments with restricted access controls to ensure that only authorised personnel can access system data. Passwords are stored using industry-standard encryption methods, and sensitive operations—such as profile changes, CV uploads, and job submissions—are protected by secure session technology. We also employ firewalls, multi-layered server security, and automated monitoring tools to detect suspicious activity, prevent fraud, and maintain the integrity of our platform.

We conduct regular system audits, data backups, and vulnerability assessments to ensure service reliability and compliance with UK data-protection requirements. Internal staff and contractors with access to personal data receive ongoing training in data protection and privacy best practices. Although we take all reasonable steps to safeguard user information, no online system can guarantee absolute security. Users are responsible for maintaining the confidentiality of their login credentials and for reporting any suspected unauthorized access to us immediately.

- **Data Retention Policy**
  We retain personal data only for as long as necessary to fulfil the purposes for which it was collected or to comply with legal, regulatory, and operational requirements. Employer account data and subscription information are retained for the duration of the subscription and may be kept for up to seven years thereafter to meet UK tax and accounting obligations. Candidate profiles, CVs, and job application records are stored for as long as the candidate maintains an active account. If a candidate becomes inactive, we may retain their data for a period of 12 to 36 months before securely deleting or anonymizing it, unless a longer retention period is required for legitimate business or legal purposes.

Chat messages, placement records, and notification logs are typically retained for 12 to 24 months to support dispute resolution and operational transparency. Users may request deletion of their data at any time, subject to our legal obligations to retain certain records. Once retention periods expire, personal data is either securely erased or anonymized so it can no longer be linked to an identifiable individual.

Your Rights Under the UK GDPR

As a data subject, you have several important rights under the UK General Data Protection Regulation ("UK GDPR"). These rights give you control over how your personal data is used and enable you to request certain actions from Staff Secure Ltd regarding your information. You have the **right to access** the personal data we hold about you and to request a copy of that information. You have the **right to rectification**, which allows you to request corrections to inaccurate, outdated, or incomplete data held on your account or within our system.

You also have the **right to erasure** ("right to be forgotten"), which permits you to request deletion of your personal data when it is no longer required for the purposes for which it was collected or where you withdraw consent. This right does not apply to data we must retain for legal or contractual reasons. You may request **restriction of processing** in situations where you contest the accuracy of your data, where processing is unlawful, or where you require us to retain information for legal claims. The **right to data portability** allows you to receive certain personal data in a structured, commonly used format and transfer it to another service provider.

Users also have the **right to object** to processing based on legitimate interests, including profiling related to HR or analytical processes. If we rely on consent to process your personal data, you may **withdraw your consent** at any time without affecting the lawfulness of prior processing. Requests to exercise these rights can be submitted to us using the contact details provided in this Privacy Policy. We will respond within one month, unless your request is complex, in which case we may require additional time.

Exercising Your Rights & Identity Verification

To exercise your data-protection rights, you may contact Staff Secure Ltd using the contact information provided below. When submitting a request, we may need to verify your identity to ensure that personal data is not disclosed to anyone who does not have the legal right to access it. Verification may involve confirming information already held in your account or requesting additional identification where necessary. We will never request unnecessary details, and any identification information submitted for verification purposes will be handled securely and only for the purpose of processing your request.

We aim to respond to all valid requests within one month. If a request is particularly complex or involves a large volume of data, we may extend the response period by an additional two months, as allowed under the UK GDPR. In such cases, you will be notified of the delay and the reason for it. There is generally no fee for exercising your rights; however, we may charge a reasonable administrative fee if a request is clearly unfounded, repetitive, or excessive, or we may decline to act on such requests under these circumstances.

- **Complaints and ICO Contact Information**
  If you have concerns about how Staff Secure Ltd processes your personal data, we encourage you to contact us first so we can address the matter promptly. You have the right to lodge a complaint with the UK's supervisory authority for data protection, the **Information Commissioner's Office (ICO)**, if you believe your rights have been violated or if you are dissatisfied with our response. Complaints can be submitted through the ICO website at **www.ico.org.uk**, by telephone, or by written correspondence. The ICO has the authority to review complaints, investigate data-protection breaches, and issue guidance or enforcement actions when required.

Contacting the ICO does not affect your ability to seek remedies through the courts or any other appropriate legal channels. Staff Secure Ltd is committed to maintaining a

transparent and cooperative relationship with regulatory authorities and ensuring compliance with all applicable data-protection standards.

- **Contact Details**

  If you have questions about this Privacy Policy, require assistance with your personal data, or wish to exercise any of your rights under the UK GDPR, you may contact Staff Secure Ltd using the information below. We aim to respond to all enquiries as quickly as possible and provide clear guidance regarding your rights, our data-handling practices, and any aspects of this Policy that require clarification.

Data Controller:
Staff Secure Ltd
124–128 City Road
London
EC1V 2NX
United Kingdom

Email: support@staffsecure.ai (or your preferred support email)

Users should note that email communication may not always be fully secure, and information of a sensitive nature should only be shared when appropriate and with caution. If we introduce a secure in-platform support channel or additional contact methods, these will be published on our website or user dashboard.

- **Changes to This Privacy Policy**

  We may update this Privacy Policy from time to time to reflect changes in our business operations, legal obligations, or platform functionality. Any updates will be published on this page with an updated “Last Updated” date. Material changes—such as modifications to the categories of data we collect, updates to legal bases for processing, or changes in how candidate CVs are shared—will be communicated to users through email notifications or platform alerts, where appropriate. We encourage users to review this Privacy Policy regularly to stay informed about how their personal data is handled.

Continued use of our platform after changes have been published represents acceptance of the updated Policy. If you do not agree with any part of the revised Privacy Policy, you must discontinue using the platform and may request deletion of your account and associated personal data.