

PRIVACY POLICY

Company Name: Staffs Tech Ltd

Last Updated: January 2025

ICO Registration Number: ZB288444

Version: 2.0

1. Introduction & Scope

Staffs Tech Ltd is fully committed to protecting and respecting your privacy in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This policy details how we collect, manage, use, and secure personal data across our business operations.

Important Operational Distinction for IT Clients:

As an IT Managed Service Provider (MSP), Staffs Tech Ltd operates in two distinct legal capacities:

- **Data Controller:** For the personal data of our corporate clients' business contacts, prospects, website visitors, and marketing subscribers.
- **Data Processor:** For all end-user data hosted, backed up, managed, or accessed on behalf of our corporate clients during the delivery of remote monitoring, helpdesk support, cloud hosting, and disaster recovery services.

Where we act as a Data Processor, our processing activities are strictly bound by the Data Processing Agreement (DPA) integrated into our master commercial contracts.

2. Information We Collect

We process various categories of personal data depending on your relationship with us:

- **Identity & Contact Data:** Full name, job title, corporate email address, billing address, and phone numbers.
- **Technical & System Data:** IP addresses, corporate device naming conventions, operating system versions, browser types, and localized network event logs gathered via our Remote Monitoring and Management (RMM) infrastructure.
- **Service & Support Data:** IT support desk tickets, engineering notes, diagnostic metadata, remote desktop access session records, and audio recordings of telephone support queues.

- **Usage & Marketing Data:** Information detailing how you interact with our administrative portals, customer support platform, corporate website, and your specific marketing communication preferences.

3. Lawful Basis for Processing

We only collect and process personal data where there is a valid lawful basis recognized under Article 6 of the UK GDPR. The core processing activities deployed within our MSP operations include:

Data Category	Purpose of Processing Activity	UK GDPR Lawful Basis
Identity, Contact & Support Data	Client onboarding, technical infrastructure provisioning, responding to helpdesk tickets, and fulfilling service level agreements (SLAs).	Performance of a Contract
Technical, System & Log Data	Proactive cybersecurity monitoring, patch deployment, network vulnerability analysis, threat mitigation, and infrastructure performance optimization.	Legitimate Interests (Ensuring robust network and information security)
Identity & Financial Records	Corporate invoicing, service usage audits, statutory tax compliance, and commercial fraud prevention.	Legal Obligation
Marketing & Usage Data	Distribution of tech security advisories, newsletters, or strategic IT service updates.	Consent (or 'Soft Opt-In' for active commercial accounts)

4. Data Security Controls

As a professional IT security and infrastructure provider, Staffs Tech Ltd implements rigid technical and organizational safeguards to ensure data integrity and prevent unauthorized breach, alteration, or disclosure:

- **Access Restrictions:** Enforced Least-Privilege access models across all systems. Administrative access to client environments requires mandatory Multi-Factor Authentication (MFA) paired with Role-Based Access Control (RBAC).

- **Cryptographic Safeguards:** Personal data and operational assets are fully encrypted both in transit utilizing TLS 1.3 encryption protocols and at rest using AES-256 standards across all local infrastructure and backup endpoints.
- **Vendor Verification:** Comprehensive technical vetting is executed on all foundational MSP utility sub-processors (including PSA, RMM, documentation vaults, and automated backup nodes) to guarantee total compliance alignment.
- **Workforce Governance:** All personnel undergo continuous, mandatory compliance training covering data protection legislation, secure data management, and cyber threat awareness.

5. Data Sharing & Sub-Processors

We do not trade, lease, or sell personal information. To fulfill our commercial managed service obligations, data may be shared under strict legal terms with checked sub-processors within the following domains:

- **Cloud Infrastructure Ecosystems:** Core enterprise platforms including Microsoft 365, Azure, and Amazon Web Services (AWS).
- **Specialist MSP Operational Software:** Third-party utilities dedicated to ticketing infrastructure (PSA), endpoint management tools (RMM), and encrypted configuration repositories.
- **Professional Corporate Advisory:** External accountants, statutory legal partners, regulatory auditors, and corporate cyber insurance underwriters.

All utilized third-party processors are strictly contractually bound to execute processing solely under written instructions via Data Processing Agreements (DPAs) fully compliant with UK GDPR Article 28.

6. International Data Transfers

We prioritize storing and processing personal data explicitly within the borders of the United Kingdom or the European Economic Area (EEA). In limited instances where specialized SaaS utilities route secondary metadata via overseas servers (such as US-based support hubs), we ensure safety through:

- Verifying active vendor certifications held under the official **UK Extension to the EU-U.S. Data Privacy Framework**
- Executing formal **International Data Transfer Agreements (IDTAs)** or standard contract clauses supplemented by localized Transfer Impact Assessments (TIAs).

7. Retention Protocols

Personal data is retained only for the duration required to satisfy original collection objectives, including statutory legal, financial auditing, or corporate reporting criteria. Standard ticket logs, historic configuration

archives, and remote support metadata are preserved for a standard operational period of 6 years post-contract termination to protect against latent structural disputes.

8. Your Statutory Legal Rights

Under the UK data protection framework, data subjects hold explicit statutory protections:

- **Right of Access:** Obtain verified confirmation and custom copies of your processed personal data (Subject Access Request).
- **Right to Rectification:** Demand immediate correction of inaccurate or incomplete informational datasets.
- **Right to Erasure:** Request permanent removal of records where no overriding legal basis for processing exists.
- **Right to Object/Restrict:** Terminate processing on grounds relating to your specific situation or halt profiling.

Data subjects may exercise these options at any time. If you believe your data has been handled incorrectly, you hold an explicit right to file a formal grievance with the Information Commissioner's Office (ICO) via www.ico.org.uk.

9. Web Cookies & Digital Marketing

- **Cookies:** Our online portals deploy essential core cookies required to enable system functionality. Optional analytics or tracking scripts are fully blocked until affirmative consent is given via our cookie management interface.
- **Marketing Control:** Users can revoke electronic marketing privileges instantly at any stage by interacting with the 'Unsubscribe' mechanism inside correspondence or sending an explicit request to our compliance queue.

10. Corporate Contact Information

For any inquiries, structural balance updates, or to exercise your statutory rights, please correspond directly with our internal compliance team:

Company Name:	Staffs Tech Ltd
Email Inbox:	info@staffs-tech.com
Postal Office:	Staffs tech Ltd

	Unit F11 Genesis Business Centre Innovation Way Stoke on Trent ST6 4BW
Contact Line:	03300165568