TRISET LTD · GOVERNANCE & COMPLIANCE

Privacy Policy

How Triset Ltd collects, uses and protects personal data under UK GDPR: clients, website visitors, engineers and data-bearing equipment.

Triset Ltd

Company No. 17116041 · Stretford, Manchester M32 8PS, United Kingdom
triset.co.uk · Info@triset.co.uk

VERSION 1.0 · NOVEMBER 2026

Privacy Policy

TRISET LTD · GOVERNANCE & COMPLIANCE POLICY

How Triset Ltd collects, uses and protects personal data — across our website, our IT services and our secure disposal operations.

Document	Privacy Policy
Owner	Triset Ltd (Company No. 17116041) - Stretford, Manchester M32 8PS, UK
Version	1.0 - November 2026
Classification	Public - may be shared with clients, suppliers and portal reviewers

1. WHO WE ARE

Triset Ltd ("Triset", "we", "us") is a private limited company registered in England and Wales (Company No. 17116041), providing IT field services, desktop and end-user support, IT dispatch and secure IT asset disposal (ITAD) across the United Kingdom.

For the purposes of UK GDPR and the Data Protection Act 2018, Triset Ltd is the data controller for personal data collected through our website and business operations, and acts as a data processor when handling data-bearing client equipment under instruction from our clients.

Triset Ltd is registered with the Information Commissioner's Office — registration no. ZC259459.

Fahad Nazeer, Founder — Triset Ltd Email: Info@triset.co.uk | Tel: +44 7491 569294 Manchester, M32 8PS, United Kingdom

2. WHAT DATA WE COLLECT

a) Website enquiries. When you contact us via our website form or email, we collect your name, company name, email address, phone number and the content of your message. Form submissions are relayed to our mailbox by FormSubmit, which processes them solely to deliver the message to us.

b) Service delivery data. When providing IT services at your premises, we may collect contact details of your staff representatives, site access information, and asset records (equipment serial numbers and locations).

c) ITAD operations data. When collecting and disposing of client equipment, we maintain asset registers including device serial numbers, certificates of erasure/destruction, waste transfer documentation and client identity records — required for legal compliance and audit trails.

d) Technical data. Our website hosting (Namecheap) may process standard server logs such as IP addresses and browser types for security and performance purposes. Our DNS and CDN provider (Cloudflare) may process connection data — including IP addresses — to protect the site from attacks and serve it reliably.

3. HOW WE USE YOUR DATA

We use personal data to:

- Respond to enquiries and provide quotes (legitimate interest / contract)
- Deliver contracted IT services and field engineering work (contract)
- Fulfil legal obligations as a registered waste carrier and data processor — including record-keeping, certificates and waste transfer documentation (legal obligation)
- Maintain business records, invoices and accounts (legal obligation / legitimate interest)
- Improve our services and website (legitimate interest)

We do not sell, rent or trade personal data to third parties for marketing purposes. We send no marketing emails unless you have explicitly asked to receive them.

4. DATA HANDLING IN IT ASSET DISPOSAL (ITAD)

When clients entrust us with data-bearing equipment, we act strictly as a data processor under their instruction:

- Equipment is stored securely and access is restricted to authorised personnel
- Data is erased using certified software meeting recognised UK sanitisation standards, or media is physically destroyed
- Certificates of Erasure or Destruction are issued per device, with serial numbers, method and date
- Full chain of custody is documented from collection to final disposal
- Waste is transferred only to authorised treatment facilities via registered waste-carrier documentation
- A Data Processing Agreement (DPA) is available and can be signed with clients prior to engagement, defining scope, responsibilities and liability

Where equipment contains data that cannot be reliably attributed or instructed upon, we default to secure erasure or destruction before any recycling or resale.

5. DATA SHARING

We share personal data only where necessary:

- Service providers: website hosting (Namecheap), DNS and CDN (Cloudflare), contact-form delivery (FormSubmit — relays website form submissions to our mailbox), email services — bound by their own GDPR obligations
- Authorised treatment facilities (AATFs): for e-waste processing, limited to documentation legally required (waste transfer notes)
- Authorities: where required by law, e.g., Environment Agency record-keeping, HMRC, or law enforcement with lawful basis

All data is stored and processed within the UK or under adequacy arrangements. We do not transfer personal data outside UK GDPR protections.

6. DATA RETENTION

- Enquiry correspondence: retained up to 24 months, then deleted
- Client service records, invoices, asset registers: 6 years (HMRC/company law requirement)
- Waste transfer notes and ITAD certificates: minimum 2 years (waste regulation requirement); certificates retained per client agreement
- Website server logs: retained by our hosting provider for up to 30 days

7. YOUR RIGHTS

Under UK GDPR you have the right to: access your personal data; rectify inaccurate data; request erasure; restrict or object to processing; data portability; and withdraw consent where processing is consent-based. You may also complain to the Information Commissioner's Office (ico.org.uk).

To exercise any right, email Info@triset.co.uk. We respond within one month, free of charge.

8. COOKIES

Our website uses no advertising or tracking cookies. Only strictly necessary technical cookies/local storage may be used for site functionality. We do not run analytics, advertising pixels or third-party trackers at this time. Should this change, this policy and a consent notice will be updated accordingly.

9. SECURITY

We apply appropriate technical and organisational measures: encrypted website connections (HTTPS/SSL), restricted access to records, secure handling procedures for data-bearing equipment, and staff confidentiality obligations. Where incidents affecting personal data occur, affected individuals and the ICO are notified as legally required.

10. CHANGES TO THIS POLICY

We may update this policy as our services or the law evolve. The latest version is always published on this page with its review date.

11. REVIEW DATE

This policy was last reviewed: November 2026. Next scheduled review: November 2027.