Data Protection

Background/Summary

Red Trouser Day is committed to operating transparently, securely, and in full compliance with the Data Protection Act 2018 and UK GDPR. This internal Data Protection Policy outlines how our trustees, staff, and volunteers must handle personal information. It directly operationalises the commitments made in our public Website Privacy Policy to ensure consistency between our external promises and our daily internal operations.

1. Scope

This policy applies to everyone associated with Red Trouser Day, including:

- Trustees
- Volunteers
- Contractors or consultants
- Partners and suppliers
- Anyone representing or working on behalf of the charity

2. Permitted Data Collection Categories

Volunteers and staff are strictly authorized to collect, store, and process only the categories of data declared in our privacy notice. No additional personal data should be gathered without explicit authorization from the Board of Trustees. The permitted categories are:

- Website Forms & Subscriptions: Names, email addresses, and communication preferences captured via www.redtrouserday.com for newsletters, campaigns, and event updates.
- Purchases & Order Fulfilment: Customer transaction records, shipping addresses, and contact items required to fulfill merchandise orders.
- Community Content: User-submitted correspondence, survey responses, and media assets including videos or still pictures explicitly posted by community members.
- Technical Analytics: System administration logs, including IP addresses, operating systems, and browser types managed strictly via automated server or cookie configurations.

3. Data Storage and Transfer Rules

3.1. Cross-Border Transfers & Storage Outside the UK/EEA

As highlighted in the RTD Privacy Policy, data collected via our website may be transferred to or stored at a destination outside the United Kingdom or European Economic Area (EEA), particularly when utilizing cloud tools or handling orders via global vendors. When executing or overseeing these processes, personnel must observe the following:

- Ensure all international cloud storage providers maintain robust, legally recognized standard contractual clauses or adequacy safeguards.
- Verify that any data processed by overseas staff or vendors (such as support desk teams or payment system operators) is bounded by clear confidentiality contracts.

3.2 Server Security & Central Storage

Save for explicit authorized operational workflows, all digital information must reside exclusively on the charity's designated secure primary servers or approved cloud systems. Local storage on personal laptops, mobile phones, or unencrypted external drives is strictly prohibited

4. Mandatory Security and Fundraising Operational Rules

All online transactions must be processed entirely by our secure, external payment processors.

Volunteers have no access to donor credit/debit card numbers. No member of the charity may request, write down, or store full card details on paper, emails, or text documents under any circumstances.

4.1 Password Integrity & Management

Access to administrative portals, email dispatch software, and server backends must be guarded by strong, distinct passwords. Credentials must never be written down, shared among team members, or re-used across personal profiles. Where available, Multi-Factor Authentication (MFA) must be active.

4.2 Public Event & Material Operations

When managing public events, fundraising drives, or receiving material submissions:

- Physical lists, ticket logs, or entry forms containing attendee details must remain supervised at all times and locked away immediately post-event.
- Community media assets (including video or still pictures) must only be hosted on public channels or site directories if explicit user opt-in or parental/guardian consent is confirmed.

5. Core Data Disclosures & Purpose Limitations

Personal records must only be deployed for the specified operational workflows outlined in Section 4 of our public notice. Data must never be traded, sold, or shared outside the clear boundary parameters below:

- Internal Charity Distribution: Data can be shared selectively among active team members only if structurally necessary to execute orders or manage authorized awareness programs.
- Authorized Marketplace Traders: When users initiate a transaction with verified marketplace traders operating directly via our web platform, only the necessary data items strictly required to fulfill that specific purchase may be transmitted.
- Statutory & Safety Escalation: Information can be disclosed if legally mandated, to assist in policing good behaviour on interactive portals, or to protect the safety, rights, and core property of Red Trouser Day, its users, and the wider public.

6. Facilitating Supporter Rights

The Data Protection Act 2018 grants individuals clear legal rights regarding their information. All personnel must assist in upholding these rights efficiently:

- Marketing Opt-Outs: Supporters have the right to halt processing for promotional campaigns. If an individual unchecked a consent box or sends an opt-out email to info@redtrouserday.com, internal systems must be updated to reflect this within 48 hours.
- Subject Access Requests (SARs): Individuals have a legal right to request a comprehensive copy of the data we hold about them. Any volunteer receiving a formal data access inquiry must immediately forward it to the Trustee Board. While the Act permits charging a reasonable cost-reflective fee if requests are manifestly unfounded or excessive, standard inquiries must be handled transparently, accurately, and within statutory deadlines.

7. Breach Response Protocol

A data breach occurs if personal information is lost, stolen, destroyed, or shared without authorisation (e.g., emailing the wrong contact sheet or losing an unencrypted volunteer laptop). If a data breach occurs or is suspected, volunteers must act instantly using this 3-step sequence:

1. **Immediate Containment:** Take fast steps to stop further exposure. For instance, if an email was sent to the wrong distribution list, ask the recipients to delete it immediately, or disconnect

a compromised cloud account.

2. **Notify the Data Lead:** Report the incident to the Chair of Trustees and any other designated trustee or Data Lead via info@redtrouserday.com within 24 hours of discovery. Provide exact details on what data categories were affected and the approximate number of individuals involved.

3. **Assessment & Legal Reporting:** The Board of Trustees will evaluate the severity. If the leak poses a material risk to individuals' rights and freedoms, the charity must report the incident to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of it.

8. Review

This policy will be reviewed annually or sooner if legal requirements change by the Board of Trustees. All approved policy updates will be shared with those affected.

RTD Policy Framework

Policy Area	Lead Policy	Linked Policies
Risk	Risk Management	SIR, AML, Anti Bribery, Safeguarding
People	Safeguarding	SIR, Complaints
Finance	Anti Money Laundering	Tainted Donations, Anti Bribery
Conduct	Conflict of Interest	Complaints, SIR , ***Data Protection***, Privacy
Information	Privacy	Acceptable IT Use, Complaints, Social Media, ***Data Protection***

SIR – Serious incident Reporting AML – Anti Money Laundering