TRF Data Protection Policy – Index

Document Control

Document Title / Reference	Data Protection Policy v1.0
Approved by	Graeme Collins, CEO
Date approved	24th March 2025
Review date	24th March 2027

Key points in this policy

- The Trail Riders Fellowship (TRF) organisation is obliged to safeguard Personal Data
- As a Group Officer (GO), 'Team TRF' volunteer or other entity handling TRF member data, you **must** comply with this Data Protection Policy
- Personal data must be:
    - Processed lawfully, fairly and transparently
    - Collected for specified, explicit and legitimate purposes [Purpose Limitation]
    - Limited to what is necessary (adequate and relevant) [Data Minimisation]
    - Accurate and kept up-to-date
    - Stored for no longer than is necessary for its purpose [Storage Limitation]
    - Processed securely [Integrity and Confidentiality]
    - Under demonstratable compliance with GDPR* principles [Accountability]
- This Data Protection Policy also outlines your rights as a Data Subject, providing additional guidance on how to manage consent, handle non-personal data (such as Intellectual Property) and raise concerns on security threats.

**GDPR = General Data Protection Regulation*

1 Purpose and scope

1.1 This Policy is an internal and external facing controlled document designed to guide members of the TRF and parties associated with the TRF, on:

- the TRF's data protection goals
- best practice for Data Protection & Data Privacy *[data classification / processing]*
- responsibilities and how acting on the best practice will help the organisation achieve the TRF's data protection goals.

Note, this document is distinct to a 'Privacy Notice' or 'Privacy Statement' which is a public/external facing document aiding transparency for data subjects on how the TRF data controller(s) handles their information.

1.2 For definitions of key terms used in this document, please see the Glossary at the end of this document.

1.3 Where a clause or comment says 'must', then this refers to an obligation for legal or compliance reasons. Where a clause or comment says 'should' then the clause is advisory.

2 Data protection goals

2.1 This section sets out the TRF's privacy goals and how meeting these goals will help the business protect data to:

- meet GDPR requirements for legal purposes (subclause 2.2)
- ensuring sensitive intellectual property and other corporate secret information is not used maliciously (subclause 2.3)
- grow the TRF data maturity in order to maximise strategic and operational competencies (subclause 2.4).

2.2 Personal data means 'any information relating to an identified or identifiable natural person'.

There are 7 key GDPR principles regarding personal data:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability.

(See Section 3.2 for more detail on these principles.)

2.3 Data and information can be seen as an 'intangible asset' i.e. something you can't physically touch. Digital photos, marketing information, strategic documents and similar may have exclusive 'Intellectual Property' (IP) rights that prevent others from reproducing or reusing the information without the permission of the person who owns the IP rights. These rights may belong to the author or creator, but if created in the course of employment they may belong to the employer. **By default, all intangible assets created for the TRF are assumed to be the property of the TRF and should be protected from unauthorised disclosure or misuse**. There are many forms of rights but the main areas relevant to GDPR are:

a) Copyright – original artistic work, computer software and similar
b) Database rights – information in a database collected and presented in a useful way
c) Copyright in databases – related to the effort gathering the material in databases

See link for further information on GDPR and IP: https://ico.org.uk/for-organisations/foi/freedom-of-information-and-environmental-information-regulations/regulation-12-5-c-intellectual-property-rights/#IP .

2.4 Data on its own is not so useful, but once data has been collated, reviewed and presented in context it can be considered ‘information’. The TRF is committed to providing training and resources to assist those handling TRF information to become more data-capable, thereby creating a more ‘data mature’ TRF community, able to carry out strategic actions more effectively.

3 Best practice for data protection

3.1 **Data Classification**: Data should be held in a format which is easy to classify in the following ways:

Public: 'Normal', 'Business' data, referring to non-sensitive information which can be provided to external parties without additional authorisation or is already in the public domain.

Confidential: 'Business Sensitive', 'Proprietary' information which must be authorised for use external to the TRF and is considered secret or restricted in some way.

Personal: 'Personally Identifiable Information' (PII), relating to living individuals, such as name, address or even someone's initials or code (such as a national insurance number) which identifies someone.

Personal Sensitive: 'Personally Identifiable Sensitive Information' refers to PII data which contains characteristics of the person such as medical records, political affiliations, religious information or other 'protected characteristics'.

The classification of information helps decide how the information is handled and stored in terms of Confidentiality, Integrity and Availability (CIA).

3.2 **Key principles for data processing**: Data must be processed in accordance to GDPR (General Data Protection Regulation) guidelines where personal and personal sensitive data is involved. Guidelines to help the processing of personal and personal sensitive information, in alignment with the GDPR key principles as part of 'privacy by design and default', are as follows:

3.2.1 **Lawfulness, fairness and transparency:** (lawful basis) Only handling a person's data for the benefit of the person, with a record of consent. Other than consent, all other lawful bases for data processing require the processing to be necessary, i.e. for specific purpose. There are a number of valid bases:

- Consent e.g. individuals agreeing to photos used on the intranet
- Legitimate Interest e.g. TRF member administration
- Public Task e.g. government administration (unlikely to be a primary basis for the TRF)
- Legal Obligation e.g. sending tax records to HMRC
- Contract e.g. receiving Trail magazine as a benefit
- Vital Interest e.g. to protect someone's life (unlikely to be a primary basis for the TRF).

(See https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/ for more information on lawful basis.)

3.2.2 **Purpose limitation:** Ensuring the data is only used for the purposes communicated through a privacy notice or similar. Participants can request their data is not processed for any reason.

3.2.3 **Data minimisation:** Only collecting information that is needed for the purpose stated. Consent is against each individual piece of data held, not taken as blanket consent.

3.2.4 **Accuracy**: Ensuring data is accurate (noting it's the data subject's responsibility to notify the data controllers of any inaccuracy or change). People can request access to their data at any time. If accuracy of data is in doubt then the information will not be used.

3.2.5 **Storage Limitation**: Only retaining data for as long as it's needed. Therefore all records will be deleted according to appropriate retention. Personal data will be held within a country in the EU or appropriate 'adequate country' where there are known data safeguards in place, unless otherwise specified.

3.2.6 **Integrity and Confidentiality:** (security) Personal data will shared only with agreed entities for the purposes stated in this policy and no sensitive personal data will be shared outside the data processors control unless agreed in advance by the person.

3.2.7 **Accountability**: Having appropriate measures and records in place to be able to demonstrate compliance.

More information on GDPR can be found here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/.

3.3 **Understanding data protection rights:** Data processors must be aware that data subjects located in the UK have the following rights under certain circumstances relating to their personal data:

3.3.1 **Right to information**: the right to be informed about the TRF's collection and use of their personal data.

3.3.2 **Right of access**: the right to request access to (and receive a copy of) their personal data.

3.3.3 **Right to rectification**: the right to have their personal data updated if it is inaccurate or incomplete.

3.3.4 **Right to be forgotten**: the right to request erasure of their personal data if it is no longer required for business purposes.

3.3.5 **Right to restrict Processing**: the right to request the restriction or suppression of their personal data.

3.3.6 **Right to object**: the right to object to the Processing of their Personal Data by the TRF.

3.3.7 **Right to data portability**: the right to obtain and reuse their provided personal data for their own purposes across different services.

3.3.8 **Right to withdraw consent**: the right to withdraw consent previously provided for the TRF to process their personal data.

3.3.9 **Automated decision-making including profiling**: the right not to be subject to a decision based solely on automated processing, including profiling which produces legal effects or significantly affects them.

3.3.10 **Right to complain**: the right to lodge a complaint with the competent data protection authorities.

3.4 Recording how personal information is collated and why

3.4.1 Personal information is provided by members (data subjects) to the TRF either directly through the membership portal or via other members acting as nominated 'data administrators' (or 'data processors') who also agree to abide by the principles above.

3.4.2 Consent is explicit, as 'opt-in' for each piece of information.

3.4.3 The primary purpose of data collection is to serve the membership.

3.4.4 The primary purposes data subject information is handled is as follows:

TRF Membership records – to ensure payment/subscription is maintained

Trail Magazine distribution – as a member benefit, including name and address

TRF employee records – financial and contractual for tax and human resource management including bank account name and number, bank sort code and other financial information as appropriate

TRF trail website user credentials – membership ID, name, role in order for users to log in and engage with TRF web content

TRF Green Road Map (GRM) user credentials – membership ID, name, role in order for users to log in and engage with TRF GRM web content

3rd Party Contacts – vendor contact details, name, phone, location in order to maintain service provision and contract management.

3.4.5 In some situations, it is, or may be necessary for the TRF to process Personal Data for purposes other than those indicated above. In doing so, the TRF relies on the necessity of such processing for the purpose of pursuing its legitimate interests, provided such interests are not overridden by the interests or fundamental rights and freedoms of the data subject.

3.4.1 Please contact Data.Protection@trf.org.uk with any questions about the operation of this policy.

3.5 Responding to a protected information incident

3.5.1 The TRF has implemented procedures to manage any suspected Personal Data incident, including personal data breaches, and will notify data subjects or any applicable regulator where legally required or otherwise appropriate to do so.

3.5.2 The TRF is subject to strict timelines for responding to a personal data breach where the rights and freedoms of affected individuals may be impacted. A Personal Data Breach has a wide definition and could include any scenario where Personal Data is:

- accessed by an unauthorised Third party (such as hacking/cyberattacks)
- sent or otherwise disclosed to an incorrect recipient
- lost or stolen
- altered without permission
- unavailable for significant periods of time (except for routine maintenance).

3.5.3 It is important that any suspected personal data breach is immediately reported to the TRF Directorship via Data.Protection@trf.org.uk .

4 Responsibilities

4.1 This section highlights the various responsibilities required to maintain the policy and how violations of the policy impact compliance and are handled by the TRF.

4.2 This Policy document is overseen by the TRF Directors and will be maintained by the CEO.

4.3 For the applicable Data Protection Laws, the Trail Riders Fellowship is the "data controller". The Trail Riders Fellowship is a Data Controller because it holds information about individuals (primarily members). It uses this information to administer membership and provide the services offered by the Fellowship.

4.4 General members and Guests handling TRF information for example suppliers under contract / Non Disclosure Agreement (NDA) are responsible for reading and adhering to this **TRF Data Protection Policy**.

4.5 Each system owner will provide training to system users on 'acceptable use' / 'terms of use', that outlines (and in some cases, restricts) the ways in which the network, website or system may be used. This is to reduce any security risk and ensure data is handled in the way intended.

Glossary

Term / Reference	Definition
Accountability	An obligation to be answerable for the outcome of a task (whether responsible / in charge of the task or not)
Availability	Enabling information access when needed
CEO	Chief Executive Officer
CIA	An approach to highlight data Confidentiality, Integrity and Availability as important aspects of Data Governance
Confidentiality	Keeping sensitive information private and secure
Data	A collection of raw unorganised facts such as test, observations, figures, symbols in paper or digital format. It can be processed to form 'information' and guide decision-making as 'knowledge'
Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, personal data
Data Classification	The practice of organising data according to pre-defined criteria, usually to assist with communicating what is important with respect to security and data privacy
Data Controller	A person or organisation who determines the purposes for which, and in the manner in which, any personal data is processed
Data Governance	Internal standards and policies that apply to how data are gathered, stored, processed and disposed of
Data Processing	Taking action with someone's personal data including collecting, saving, making changes or sharing with others
Data Subject	A living person for which information has been collected
External / External Audience	Parties not directly controlled through TRF policies such as vendors, general public
GDPR	General Data Protection Regulation, refers to the Data Protection Act 2018 which is the UK's version of the European Union's GDPR
ICO	Information Commissioner's Office, an independent authority in the UK that regulates information rights. Additional data terms can be found here https://ico.org.uk/for-organisations/advice-for-small-organisations/key-data-protection-terms-you-need-to-know/
Integrity	Ensuring information is complete and accurate, free from corruption
Internal / Internal Audience	Parties directly controlled through TRF policies including the TRF Board, Team TRF and nominated members with specific roles and responsibilities working (paid or voluntarily) on behalf of the TRF

NDA	Non Disclosure Agreement, a confidential document which acts as an agreement for a 3rd party not to use information outside agreed terms and conditions
Personal Data	Data relating to an identified or identifiable living person
Policy	Best practice guidance or principle of action
Privacy by Design and Default	A phrase used by the ICO as a legal requirement to 'bake in' awareness and procedures on how to handle personal information in all business processes, to reduce data risk to individuals' personal information
Privacy Notice	A notice setting out information that may be provided to data subjects when the TRF collects information about them. They may take the form of general privacy statements applicable to a specific group of individuals, or they may be stand-alone privacy statements covering processing related to a specific purpose
System Owner	A conceptual description of someone who has responsibility for a set of information that can be described as a single unit i.e. bounded
TRF	Trail Riders Fellowship