Date of Last Review: 28/08/2026
Date of Next Review: 28/08/2027
Version: 2.2

PRIVACY, GDPR, DATA PROTECTION & RETENTION POLICY

We're currently reviewing and updating our data retention schedule. If you have any questions in the meantime, please get in touch at info@findingyourfeet.net

Introduction

At Finding Your Feet, we're committed to handling personal data responsibly, transparently, and in line with UK GDPR and the Data Protection Act 2018. This policy explains how we collect, store, use, and share personal data.

Our Aims

- Follow UK GDPR and related data protection laws.
- Make sure personal data is used lawfully and fairly.
- Give everyone confidence that their data is safe with us.

Our Principles

We stick to the core data protection principles:

- Lawfulness, fairness, and transparency – we'll always tell people what we do with their data.
- Purpose limitation – we only use data for the purpose for which it was collected.
- Data minimisation – we collect only what we need.
- Accuracy – we keep data correct and up to date.
- Storage limitation – we don't keep data longer than necessary.
- Integrity and confidentiality (security) – data is kept safe and secure.
- Accountability – we can show how we comply with GDPR.

What We Collect and Why

We may collect:

- Names, addresses, emails, and phone numbers

- Donation and fundraising info
- Communication preferences
- Volunteer and staff information
- Supporter and event participation details

We use this information to:

- Provide services and support
- Process donations and claim Gift Aid
- Communicate with supporters and volunteers
- Manage internal HR and volunteer processes
- Meet legal and safeguarding obligations

Personal data must not be entered, uploaded to, pasted into, or otherwise processed by AI tools unless the tool has been approved for that specific purpose, the lawful basis has been confirmed, and the data has been minimised, anonymised, or pseudonymised wherever possible. Special category data, safeguarding information, minors' data, CCTV footage, audio recordings, donor records, HR records, and support case notes must not be used with AI tools unless there is a documented business need, approval from the CEO or IT Manager, and if necessary, a risk assessment has been completed.

Data Access & Rights
You have the right to:

- Request a copy of your personal data
- Have inaccurate data corrected
- Request deletion of your data
- Withdraw consent at any time

To make a request, email us at: info@findingyourfeet.net
If you ask us to delete your personal data, we will do so promptly, unless we are legally required to keep it (for example, Gift Aid or financial records).

We handle these requests in line with our internal Subject Access Request (SAR) procedure, and will respond within one month of receiving your request. If it's complex, we may extend this by up to two months - we'll let you know within the first month if that's the case, and why.

If you'd like us to review our response to a data request, please get in touch within 3 months of our last contact with you about it.

If you're unhappy with how we've handled your data, you can raise it with us at info@findingyourfeet.net. You also have the right to complain directly to the Information Commissioner's Office (ICO) at www.ico.org.uk. Our registration number is ZB255293.

Legitimate Interest
We may process personal data based on our legitimate interest in keeping supporters informed about our activities, events, campaigns, and services. This means we can contact you even if you haven't explicitly opted in, as long as it doesn't override your rights or freedoms.
You can object to this processing at any time. If you do, we will stop using your data for these purposes, unless we are legally required to keep it (for example, for Gift Aid or financial records). To object, email info@findingyourfeet.net or use the unsubscribe link in our communications.

Third-Party Services
We work with trusted platforms (e.g., PayPal, Stripe, Beacon CRM, Active Campaign) to help us deliver services. We only share the minimum data required, and we must confirm that each partner has appropriate GDPR-compliant privacy, security, retention, deletion, audit, and subcontractor controls before personal data is shared. Where a platform includes AI features, those features must be assessed and approved before use with personal data, and any AI processing must be limited to the purpose we have authorised.

In some cases, we may collect sensitive personal data (known as "special category data"), such as health information, to provide support services or meet safeguarding obligations. We only do this with consent or where it is necessary for reasons of substantial public interest, in line with UK GDPR regulations and the Data Protection Act 2018.

CCTV & Audio Recording
We use CCTV in our car park and a Ring camera in our reception area (which records both video and audio) to help keep our building, staff, visitors and property safe.
CCTV footage is stored for up to 10 days and Ring recordings for up to 180 days, unless we need to keep specific clips longer because of an incident.

Access to these recordings is limited – CCTV footage can be viewed by our Founder, CEO and FYF staff, while Ring recordings are restricted to our Founder, CEO and our Charity Hub team.
If you appear on our cameras, you can ask us about it and request a copy of the footage by contacting our Founder, CEO or Charity Hub team. Please note that to protect others' privacy, we may need to blur or remove other people's images or audio before sharing.

CCTV footage, ring camera recordings, audio recordings, and still images must not be uploaded to AI tools for transcription, identification, behavioural analysis, image enhancement, facial recognition, sentiment analysis, or automated decision-making unless there is a lawful basis, a documented necessity assessment, approval from the CEO or IT Manager, and a record of the processing. Facial recognition or biometric identification must not be used unless specifically approved following a separate risk assessment.

Data Breaches
If a personal data breach happens, we follow our Data Breach & Incident Response Policy, which sets out how we assess, contain, and respond to incidents. Where a breach is likely to result in a risk to people's rights and freedoms, we'll report it to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of it, and we'll contact anyone affected without undue delay where there's a high risk to them.

A breach may also include personal data being entered into an unapproved AI tool, disclosed through an AI prompt or output, used for unauthorised model training, retained by a vendor outside approved settings, or included in an inaccurate AI-generated record that could affect an individual.

Data Retention

We keep personal data for as long as it's needed and in ways that are safe and secure. Different types of data have different purposes, and we periodically review our records to make sure we're not holding anything longer than necessary.

Retention reviews include copies of personal data held in approved systems, exports, backups, AI prompts, AI outputs, transcripts, summaries, and temporary working files where those records contain or reveal personal data.

Data Retention Schedule

Where a retention period is required by law, this overrides a request for erasure under UK GDPR

Category of Data	Details	Retention Period	Disposal Activity
Service Users ('Troopers')	Sensitive personal data, needed for support and follow-up	Retained for as long as necessary to provide support.	Paper: professionally shred. Electronic: anonymise
Fundraisers, donors & event attendees	Names, addresses, emails, phone numbers	Retained for as long as necessary to process donations and maintain the relationship. Legal obligations to keep for 6 years in certain circumstances (eg Gift Aid).	Paper: professionally shred. Electronic: anonymise
Contact Forms (website)	Names, emails, addresses	Retained for as long as necessary to respond or follow up.	Electronic: anonymise
Emails (marketing / communications)	Names, email addresses	Retained for as long as necessary to manage communications.	Electronic: delete or anonymise when no longer needed

E-Newsletter Subscribers	Names, email addresses	Retained until the individual unsubscribes or withdraws consent.	Electronic: remove from mailing list

Key Points

- Anonymisation vs Deletion: Anonymised data cannot be linked back to anyone.
- Minors' Data: Extra care is taken to meet safeguarding obligations.
- Consent & Legal Obligations: We review relationships and consent periodically, and keep legally required records (Gift Aid, financial info) for 6 years.
- Exceptions: Any deviation from these general retention practices must be approved by the CEO and documented.

Sharing Personal Information & Consent

We only share personal data when it's necessary, appropriate, and lawful. In most cases, we'll ask for clear consent - especially for sensitive info like health details or personal stories. This may include sharing data with partner organisations, healthcare providers, or funders, but only with permission, unless the law or safeguarding duties require otherwise. We make sure sharing is secure and respectful of everyone's rights and privacy.

This policy should be read alongside our AI Acceptable Use Policy, which sets out additional rules for using AI tools with personal data.