



Information Security & Data Protection Policy

Created: January 2026

1. Purpose and Scope

Spread Some Sunshine relies on volunteers and Trustees working remotely, using personal devices and online tools, to run its social media, communications, fundraising and administration. This policy sets out how everyone acting on behalf of the charity should handle information and data securely and applies to all Trustees and volunteers, including anyone with access to the charity's accounts, email, social media, or supporter/beneficiary information.

2. Roles and Responsibilities

- The Trustees are collectively responsible for information security and data protection.
- Faye Toner (Founder & Trustee) is the point of contact for reporting any data or security concerns.
- Every volunteer and Trustee is responsible for following this policy when using their own devices, accounts or platforms for charity business.

3. Personal Data and Confidentiality

The charity holds personal data about supporters, donors, volunteers and the charities/organisations it supports. This data must only be used for legitimate charity purposes, in line with UK GDPR.

- Only collect and keep the personal data that is actually needed.
- Never share supporter, donor, volunteer or beneficiary personal details outside the charity without authorisation from a Trustee.
- Take particular care with any information relating to children or vulnerable people - this should only be shared on a strict need-to-know basis.
- Do not download or store personal data on personal devices any longer than needed to complete a task.

4. Devices, Passwords and Account Security

- Use a strong, unique password or passphrase for every charity-related account (email, social media, Canva, Mailchimp, Stripe, Enthuse, etc.) and enable two-factor authentication where it's available.
- Never share login details for charity accounts by email or messaging apps; use a password manager or agree a secure handover process where access must change.
- Keep phones, laptops and tablets used for charity work locked with a passcode, PIN, or biometric lock and keep their software up to date.
- Log out of shared or public devices after use and avoid accessing charity accounts on public computers.

5. Working Remotely

- Most charity work is done remotely - take reasonable care to keep devices and screens away from unauthorised view when working in public places.
- Avoid accessing sensitive charity information over unsecured public Wi-Fi where possible.
- Report a lost or stolen device that has access to charity accounts to a Trustee immediately, so passwords can be changed.

6. Email and Acceptable Use

- Use charity email/communication channels for charity business in a manner consistent with the charity's values.
- Be cautious of unexpected emails, links or attachments, even from familiar-looking senders - do not enter charity login details into a link received by email.
- Do not use charity accounts or platforms for personal, offensive or unlawful purposes.

7. Payments and Financial Data

Spread Some Sunshine does not take or store payment card details directly. All donations and ticket sales are processed through Stripe and Enthuse, which handle card data under their own security standards.

- Never ask a donor or supporter to send card details by email, text or social media message.
- Never write down, photograph or store anyone's card details.
- Direct any payment queries to the charity's Stripe/Enthuse account holders rather than handling card data manually.

8. Third-Party Platforms and Data Processors

The charity uses a small number of trusted online platforms to carry out its work, including:

- Stripe and Enthuse - donations and event ticketing/payment processing
- Mailchimp - email newsletters and supporter communications
- Canva - design and content creation
- Instagram and Facebook - social media

Only these or other Trustee-approved platforms should be used to handle charity data. New tools or platforms that will handle supporter or beneficiary data should be agreed with a Trustee first.

9. Data Retention and Disposal

- Keep personal data only for as long as it's needed for the purpose it was collected.
- Securely delete files, emails, or contact lists that are no longer needed, rather than leaving them on personal devices indefinitely.
- Financial records are retained for at least six years in line with the Financial Controls Policy.

10. Reporting an Incident or Data Breach

If you suspect a charity account has been compromised, a device with charity access is lost or stolen, or personal data has been accidentally shared, lost, or exposed, report it immediately to Faye Toner or another Trustee.

- Early reporting matters - the Trustees may need to assess whether the Information Commissioner's Office (ICO) must be notified within 72 hours under UK GDPR.

- No one will be penalised for reporting a genuine mistake promptly.

11. Review

This policy will be reviewed annually by the Trustees to ensure it remains appropriate and reflects the platforms and ways of working actually in use.

Approval

This policy has been reviewed and approved on behalf of the Trustees of Spread Some Sunshine.

Electronically signed:

Faye Toner

Faye Toner

Founder & Trustee, Spread Some Sunshine

Date: January 2026

Next scheduled review: January 2027