

Privacy Notice and Data Protection Policy

Policy date
31 March 2026

Next review
31 March 2027

Policy owner
Board of Trustees

Version
2.4 - 22 October 2026

PRIVACY NOTICE

1. Who we are and how to contact us

This notice explains how Roots for Change UK CIO uses personal information when you use our services, support us or work with us. We are a Charitable Incorporated Organisation registered in England and Wales, charity number 1209308, and the controller responsible for the uses described here. Our registered office is Bargain Outlet, 111-113 King Street, South Shields, Tyne and Wear, NE33 1DP.

To ask a question, exercise your rights or raise a concern, email info@rootsforchangeuk.com, call +44 7960 287537 or write to the address above. Ask for the Data Protection Lead or, if your concern involves that person, a trustee with no conflict of interest. We can help explain this notice in an accessible format. For sensitive information, ask for a private conversation or secure way to send it.

Only the information relevant to your contact with us applies to you. The first part explains our uses of information and your choices. The internal procedures and Annexes A and B set out the rules our trustees, staff and volunteers must follow, including how long records are kept.

2. What we collect and where it comes from

We receive information from you when you contact us, join an activity, volunteer, donate or raise a concern. We may also receive relevant information from a parent or authorised representative, a referee, a referral or delivery partner, a payment provider or statutory services. We will explain the source and use unless a lawful exception applies. A referral does not give permission to use your information for unrelated publicity or marketing.

What we need depends on the activity. It may include contact details, age or date of birth, household or emergency-contact details, attendance, support needs, limited evidence of eligibility, volunteer applications and checks, donations, Gift Aid, complaints or safeguarding records. We collect health, ethnicity or other sensitive details only when needed for a stated purpose, with the extra safeguards explained below. We do not ask everyone for all of this information.

For website visits and donations, records may include payment status and reference, amount, date, refunds or subscriptions, and limited technical or security information. Stripe handles card details on its payment pages. Our staff must not collect or store full card numbers or security codes in charity records.

3. Why we use your information

Data protection law requires a lawful basis for each use of personal information. The table sets out the bases for our activities. Where we rely on legitimate interests, we must record why the use is necessary and proportionate, balance it against your rights, and use a less intrusive option where one will achieve the same purpose. We rely on a legal obligation only where a specific duty applies.

Purpose and relevant information	Lawful basis and limits
Responding to enquiries; contact details and the information you provide	Legitimate interests in answering requests, maintaining useful communications and running the charity responsibly.
Organising requested activities and support; registration, attendance, referrals, relevant household or eligibility details	Legitimate interests in providing and evaluating accessible support, coordinating participation and maintaining safety. Collect only what the particular service needs; additional conditions apply to sensitive information.
Volunteer recruitment and management; applications, references, role checks, training and placement records	Legitimate interests in fair selection, safe delivery, supervision and accountability. Apply a specific legal duty only where it actually applies; criminal-record information requires a separate lawful condition.
Donations and donor support; payment references, preferences, receipts, subscriptions and refunds	Legitimate interests in administering donations, responding to donors and protecting charity funds. Optional donor messages must not be reused for publicity without an appropriate separate basis.
Gift Aid, accounting and regulatory records	Applicable tax, charity and accounting obligations; legitimate interests in accurate records where no specific duty requires the particular information. Gift Aid information is used only for a valid claim and related administration.
Safeguarding, serious incidents, fraud prevention and legal claims	Necessary legitimate interests in protecting people and charity assets, or a specific applicable legal obligation. Vital interests may apply in an emergency where necessary to protect life. Sensitive and criminal-offence information needs the additional conditions below.
Complaints and rights requests	Legitimate interests in resolving service complaints fairly; applicable data-protection duties for rights requests and complaints about personal information. Keep only evidence needed for the issue and a proportionate accountability record.
Optional images, publicity, fundraising messages and optional website measurement	Consent for optional identifiable publicity and optional measurement where required. Unsolicited electronic marketing to individuals uses consent by default; any lawful alternative must meet the documented conditions in the marketing section.
Employment or supplier administration, where applicable	Necessary steps for or performance of the relevant contract, and applicable employment, tax or other legal duties. This does not mean that a volunteer placement is an employment contract.

4. Sensitive information and safeguarding

Sensitive information needs an additional legal condition. For an optional adjustment or publicity, we may ask for your explicit consent under Article 9(2)(a) of the UK GDPR. We must explain the purpose and give you a real choice. Refusing optional publicity or marketing does not affect essential support. Other conditions may apply, including legal claims under Article 9(2)(f), or protecting life under Article 9(2)(c) where the person cannot give consent and the legal tests are met.

When protecting a child or an individual at risk, we may rely on Article 9(2)(g) and Schedule 1, paragraph 18 of the Data Protection Act 2018. The Data Protection Lead must record how the particular case meets the safeguarding and substantial-public-interest tests, including why information needs to be used without consent. Annex B sets out the safeguards and records required.

Criminal allegations, convictions and offence-related checks require both an Article 6 basis and authorisation under Article 10. Where we have no official authority, this normally means an applicable Schedule 1 condition. The lead must record that condition and the required safeguards before the information is used. The charity must also check separately whether the role is eligible for a DBS check.

We must explain information use to children in language they understand, taking account of their maturity, views, safety and the authority of anyone acting for them. Staff must share necessary safeguarding information lawfully and promptly. Uncertainty about consent must not delay protection. The safeguarding and data leads must check and follow any statutory sharing duty that applies to the charity's role, including section 16LA of the Children Act 2004 where within scope, and the current statutory guidance.

5. What you need to provide and what is optional

Our online donation process needs an email address to confirm and support your payment. Gift Aid is optional, but we need the required donor details and declaration to make a valid claim. For volunteering or a service, we may need essential contact, role or safety information. We will explain why and consider an alternative if you cannot provide it.

Please send only the information we need. We should check eligibility or suitability using the minimum evidence and avoid keeping document copies where a brief verification record is enough. You do not need to send complete medical histories or unnecessary details about other people. Photography, donor messages and marketing choices are separate from access to essential support.

6. Who we share information with

We share information only where it is needed for the relevant purpose. Our website and donor services include Stripe for payments, subscriptions and refunds; Monday.com for contact and volunteer forms; Google measurement or advertising services where you give the relevant consent; and website hosting, WordPress and email providers. HMRC receives information for eligible Gift Aid claims. Some providers process information on our instructions; others also have separate responsibilities as controllers.

Where necessary and lawful, we may share information with authorised delivery or referral partners, safeguarding services, police, regulators, insurers or professional advisers. Funders should receive anonymous or combined information where that meets their reporting needs. Staff must have a specific lawful reason, and provide the required privacy information, before sharing identifiable records. A request from a donor or partner is not enough on its own.

Our website rules limit Google Ads donation reporting to a signal that a donation was completed and a reference used to prevent duplicate counting. That event must not contain donor identities, contact details, Gift Aid details, payment details, campaign preferences or donation amounts. Our website privacy and cookie notices give more detail; you can also request copies from us.

7. Information sent outside the UK

Some service providers may process information outside the UK. An authorised overseas activity may also involve sharing information with a delivery partner. Before a restricted transfer, the Data Protection Lead must check the recipient, purpose, information and legal route. This may involve UK adequacy regulations, appropriate contractual or other safeguards, or a limited exception where its conditions are met.

Where we rely on Article 46 safeguards, the lead must complete the required transfer risk assessment or data protection test and arrange any additional protection before the transfer. Consent to receive a service, or a supplier's privacy notice, does not by itself provide these safeguards. Contact us to ask about a transfer affecting you or to request a copy of its safeguards, subject to lawful limits on disclosure.

8. Photographs, messages and website choices

Before using an identifiable photograph or personal story, we must explain where and how it will be used, obtain the required permission and check safeguarding risks. A child's discomfort or objection must be respected even if a parent has agreed. Where we rely on consent, you can withdraw it through the contact routes above. We must stop future use and explain any practical limits on recalling material already lawfully distributed.

You can ask us to stop direct marketing, including fundraising messages, at any time. We must honour that request. We use consent as the default for email or text marketing to individuals. The charity soft opt-in can be used only for details collected directly on or after 5 February 2026 through interest in or support for our purposes, with an opt-out offered at collection and in every message. Those messages must solely further our charitable purposes. The lead must record every condition and the relevant legitimate-interest assessment. Receiving essential support does not, by itself, give permission for marketing.

Our website offers choices for optional Google Analytics and Google Ads measurement. The cookie notice explains donation security and confirmation technologies and external Monday.com forms. Loading an embedded form can send connection information to Monday.com. Staff must ensure that non-essential cookies or similar technologies requiring consent do not operate before it is given. You can change your optional choices or contact us for another way to make an enquiry.

9. Your rights

Depending on the circumstances, you can ask to see or correct your information, have it erased, limit its use, or receive a portable copy. You can withdraw consent without affecting earlier lawful use. We may need to retain some information for a legal duty, safeguarding need or legal claim. If we cannot fulfil a request in full, we will explain the lawful reason.

You can object to direct marketing at any time and we must stop it. You can also object to a use based on legitimate interests because of your particular situation. We must consider the objection and stop unless the law permits continued use, for example because of overriding grounds or legal claims.

Contact us verbally, by email, by post or through another available channel. You do not need a special form or legal wording. We may make proportionate checks of your identity or authority where

necessary. There is normally no fee. We normally answer access requests without undue delay and within one month. The internal procedure explains when the law allows an extension or a pause.

10. If you are unhappy with how we use your information

Please contact info@rootsforchangeuk.com, +44 7960 287537 or our postal address and ask for the Data Protection Lead. If your concern involves that person, ask for a trustee with no conflict of interest. We aim to acknowledge your complaint within five working days and must do so within 30 calendar days. We must make appropriate enquiries, keep you informed and explain the outcome without undue delay. Our usual response target is 20 working days; if we need longer, we will explain why and provide updates.

You can also complain to the Information Commissioner's Office (ICO). Call 0303 123 1113 for information about its complaints process. You do not need our permission. Our Complaints Policy explains how to request an impartial review. A complaint does not change the separate deadline for a request to exercise your data rights.

11. Automated decisions and changes to this notice

Our website and donation service do not use personal information for decisions made solely by automated means that have legal or similarly significant effects. Before another service introduces profiling or automated decisions, the Board must check the legal conditions, assess the risks, put the required safeguards in place and update the relevant notice.

The Data Protection Lead must review this document and collection notices when services, suppliers, purposes or the law change. Where required, we will explain a material new use before it begins.

INTERNAL DATA PROTECTION PROCEDURES

12. Responsibilities and records

The Board is responsible for data protection. It must assign a Data Protection Lead and an alternative for absence or conflicts. An unconflicted trustee carries out the role until a separate appointment is made. The Board must also assess whether a statutory Data Protection Officer is required; the lead role alone does not fulfil that requirement. Anyone answering a public contact channel must forward requests and incidents promptly and confidentially.

Keep a processing record for each activity: its purpose; the information and people involved; source; Article 6 basis and any Article 9 or Article 10 condition; recipients; systems; access owner; transfer route; privacy notice; retention; and security measures. Carry out a data protection impact assessment before new high-risk processing and consult the ICO where unresolved high risk legally requires it. For information received from another source, give the required notice normally within one month, or earlier where first contact or disclosure requires it, unless a documented legal exception applies.

13. Security and suppliers

Limit access to authorised roles. Use individual accounts and multi-factor authentication where available, protect devices and transfers, and keep sensitive records separately with restricted access. Do not use personal accounts, open sharing links or unapproved online or AI tools for charity personal information. Arrange secure backups and recovery checks appropriate to the risk. Remove access promptly when duties end and train people before they handle sensitive records.

Before using a processor, check security, sub-processors, deletion and international transfers, and agree the required processing terms. Check how cookies and forms actually behave. Record sharing decisions and verify the recipient before sending sensitive information. Necessary safeguarding disclosures must be lawful, prompt and limited to the information and method needed.

14. Handling requests to exercise rights

Log the original receipt date, request, safe contact method and handler; identify the right being exercised and its legal deadline. Make necessary identity or authority checks promptly. Search reasonably and proportionately, preserve relevant information and consult affected record owners without disclosing more than needed. Consider third-party information and any exemption individually, with reasons recorded.

For subject access, the normal deadline is one month from receipt, or the legally relevant receipt of necessary identity information or a permitted fee. An extension of up to two further months may apply for complexity or multiple requests from the same person; explain the reason within the initial month. Pause the access-response clock for clarification only when reasonably required under the current rules, recording the request and reply dates. Internal delay or workload alone is not a lawful pause.

Send the response securely in an accessible format. Explain any refusal or restriction and the person's complaint and challenge rights. Record information supplied, exemptions, response date, any correction or deletion, and the retention review date for the case. Use Complaints Policy for a complaint about handling; keep the request's statutory deadline separate.

15. Data incidents and breaches

Report loss, misdirected disclosure, unauthorised access, alteration or unavailability immediately to the Data Protection Lead or an unconflicted trustee. Contain the incident safely, preserve evidence and record when the charity became aware. Assess affected information, people, likely harm and protective action; do not wait for a complete investigation to consider notification.

Notify the ICO without undue delay and, where feasible, within 72 hours of awareness unless the breach is unlikely to risk people's rights and freedoms. Give information in phases if necessary and explain a late report. Where a breach is likely to create a high risk, inform affected people without undue delay unless a lawful exception applies. All breaches, including decisions not to notify, require a record of facts, risk assessment, reasons, actions and follow-up.

The lead coordinates any necessary notifications to suppliers, safeguarding services, police, insurers or funders. Trustees review the cause and make sure corrective action is completed. The 72-hour period is a notification deadline where reporting is required; the assessment must begin immediately.

Annex A - Retention and secure disposal schedule

This schedule sets the charity's normal retention periods. Follow any different period required by an applicable law or contract and record the reason. Keep only the parts of a file needed for that purpose, reviewing sensitive supporting material separately. If an investigation, claim, safeguarding need or legal hold requires longer retention, record the reason, owner and next review date.

Record the category, closure or trigger date, retention reason and expected disposal or review date. At least annually, the Data Protection Lead coordinates reviews with the finance, complaints and safeguarding leads. When information is no longer needed, delete it securely or irreversibly anonymise it, including copies and exports under the charity's control. Manage backup expiry so deleted information does not return to routine use.

Record category	Default period or decision criteria	Owner
Financial, donation, refund, expense and Gift Aid evidence	Keep required financial records for at least six years after the relevant accounting period. Retain only the necessary tax and accounting evidence; record any longer specific legal or grant requirement and remove unnecessary supporting personal details earlier.	Finance lead / trustee
Unpaid abandoned online checkout identifiers	Anonymise after 30 days, except a limited record needed for a documented incident or claim.	Website / data lead
Donor message attached to a donation	Remove after one year unless separately needed for a recorded complaint or legal matter.	Fundraising / data lead
Routine enquiries	Normally 12 months after resolution, then delete or anonymise unless an ongoing relationship or a specific recorded obligation requires the relevant information.	Service owner
Routine activity registration and attendance	Normally three years after the last relevant activity for proportionate monitoring and accountability. Remove unnecessary identifiers earlier; retain only specific evidence required by a longer funding or legal obligation.	Activity lead
Emergency contacts and routine health or access adjustments	Keep while needed for participation and normally no more than three months after it ends. Transfer only relevant incident information to the appropriate restricted case record.	Activity / safeguarding lead

Record category	Default period or decision criteria	Owner
Unsuccessful volunteer applications	Normally six months after the decision, unless a complaint, safeguarding concern or agreed future opportunity provides a recorded reason to retain specified information.	Volunteer lead
Core volunteer placement and suitability record	Normally six years after the placement ends, limited to relevant role, dates, training, decisions and accountability evidence. Do not retain the whole contact or health file automatically.	Volunteer lead
DBS certificate information or a necessary copy	Destroy as soon as no longer needed for the decision and ordinarily within six months of it. Any longer retention needs a specific documented lawful reason and restricted access. A minimal check record may be kept without reproducing offence details.	Safer recruitment lead
Complaints and conduct case records	Normally six years after final closure, retaining only proportionate evidence. Review sensitive material at least annually; safeguarding, employment or legal requirements may change the case-specific period.	Complaints lead / trustee
Data-rights request and privacy complaint evidence	Normally three years after closure for accountability, using a minimal case record; extend only for a documented investigation or legal reason.	Data Protection Lead
Child or adult safeguarding records	Retain while risk, enquiry, review, claim or legal hold remains live. At closure, the safeguarding and data leads record the case-specific reason and expected disposal or review date, considering age, capacity, later disclosures, legal advice and statutory-service requirements. Review at intervals no longer than 12 months; do not automatically destroy at age 18 or after six years. If uncertain, preserve temporarily and obtain advice promptly.	Safeguarding and data leads
Marketing preference and suppression records	Keep current preferences while used; retain only the minimum suppression information needed to honour an objection and prevent re-contact. Review necessity annually. Keep limited evidence of the permission relied on for as long as reasonably needed to demonstrate the relevant communications were lawful.	Fundraising / data lead
Publicity images and permissions	Review at least annually and at the end of the agreed use; remove when the purpose expires or consent is withdrawn where applicable. Retain only proportionate permission or withdrawal evidence needed for accountability.	Communications lead
Security and technical logs	Use a documented risk-based period, normally no more than 90 days for routine logs under charity control; move necessary incident evidence into a restricted case record. Supplier-specific periods must be checked before use.	System owner / data lead
Processing, assessment and governance records	Keep current records and proportionate evidence of previous decisions while needed for accountability. Retain the Annex B appropriate policy document for at least six months after the relevant processing ends, and longer where necessary for a live matter.	Board / data lead

Annex B - Sensitive-data safeguards and appropriate policy document

This annex sets the safeguards for sensitive and criminal-offence information. Where a Schedule 1 condition requires an appropriate policy document, this annex fulfils that policy function. Before processing begins, the lead must record the purpose, Article 6 basis, Article 9 or Article 10 condition, why the use is necessary and how the facts meet any Schedule 1 tests. The policy does not remove the need to establish a lawful condition for each activity.

For safeguarding under Schedule 1 paragraph 18, record why the information is needed to protect a child or an eligible individual at risk, the substantial public interest, and why consent cannot appropriately be obtained. For employment or other conditions, identify the particular duty or permitted purpose and demonstrate that its tests are met.

Use information fairly and give clear privacy information unless a lawful exception is recorded. Collect only what the purpose needs, distinguish facts from allegations, correct errors, restrict access and protect storage and disclosure. Follow Annex A and record any different retention period and its reason. Keep a record of recipients and the reason for each sensitive disclosure. In an urgent safeguarding case, act promptly and lawfully and record the decision at the time.

The Data Protection Lead reviews these safeguards at least annually and when processing changes. Retain the policy and version record for at least six months after the relevant processing ends, and provide it to the ICO without charge if requested. The Board must resolve gaps in processing records or safeguards before authorising the activity.