

DATA PROTECTION & GDPR POLICY

Privacy. Dignity. Security. Accountability.

Updated: 12 October 2026 | **Previous policy:** 16 June 2026 | **Review:** annually

RFTUK must not collect, share or keep more personal information simply because technology makes it easy to do so.

1. Who we are and what this policy covers

Right First Time UK Ltd (RFTUK) is a **non-profit company limited by guarantee, company number 17493370**. For personal information whose purposes and means RFTUK determines, RFTUK is the data controller. A separate provider may act as its processor or as an independent controller depending on the service.

This policy describes the standards we apply to personal information relating to website visitors, members, subscribers, applicants, Directors, Campaign Leaders, Volunteers, supporters, service users and people who contact us with complaints or evidence. It covers relevant RFTUK services, including the Parent Contribution Service (PCS). Specific privacy notices explain particular processing in greater detail.

2. Legal framework and privacy principles

RFTUK applies the UK GDPR, Data Protection Act 2018, the Data (Use and Access) Act 2025 where in force, and the Privacy and Electronic Communications Regulations (PECR) where relevant. We review applicable ICO guidance when practices or legislation change.

Our core principles are **lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability**. Privacy must be considered when designing or changing a form, campaign, portal, AI workflow or other service.

3. Data protection responsibility and regulatory checks

RFTUK will assign responsibility for coordinating privacy enquiries, rights requests, incident response and complaints. We will assess and document whether a formal Data Protection Officer (DPO) is legally required rather than automatically using that statutory title.

We will also check whether an ICO data-protection fee is payable and, where required, complete and maintain the relevant registration/payment. Governance oversight does not make the Board itself a separate data controller.

4. What personal information we may handle

Depending on the activity, we may process names, contact details, correspondence, membership/subscription choices, payment references, applications, role and access records, conflict declarations, campaign and event activity, complaints, security logs, accessibility needs and information a person chooses to submit about their experience.

Some submissions may contain health, disability, child-related, safeguarding, financial, court, benefits or other sensitive information. **We should not request full case files, identity documents, bank details, medical records or third-party data by default.** We assess what is needed and encourage suitable redaction before documents are sent.

5. Lawful bases and consent

RFTUK must identify an appropriate **Article 6 UK GDPR lawful basis for each purpose**. Depending on the facts, this may be consent, contract, legal obligation, vital interests, legitimate interests, recognised legitimate interests where the statutory conditions are satisfied, or public task where supported by law. Describing work as charitable, safeguarding or public-interest activity is not itself a standalone lawful basis.

Where consent is used, it must be valid, recorded where appropriate and capable of being withdrawn. Where legitimate interests is used, RFTUK will assess necessity, reasonable expectations and the person's rights as required; recognised legitimate interests must meet the applicable legal conditions.

6. Special-category, criminal-offence and political data

Information about health, disability, ethnic origin, religious belief, political opinion and other **special-category data** requires an Article 6 basis and a separate Article 9 condition. Criminal-offence and allegation data is subject to additional Article 10 and Data Protection Act controls. Relevant Schedule 1 conditions may require an Appropriate Policy Document and associated records.

Political independence does not authorise building political profiles of members, donors or website visitors. A political affiliation disclosed for a genuine conflict-of-interest assessment should be limited to what is necessary and must not be repurposed for political targeting.

7. Children, safeguarding and restricted court material

Children's personal information and safeguarding material require heightened care, restricted access and risk-based review. A parent's willingness to provide documents does not automatically justify collecting or publishing information about a child or another adult.

Family-court material may be subject to reporting restrictions or orders. We should seek redacted or summarised information wherever suitable, and no one may assume that possession of a document means it can lawfully be published. Safeguarding disclosures may require proportionate sharing with appropriate authorities; absolute confidentiality cannot be promised.

8. Members, subscribers, donations and organisational records

We use relevant information to administer membership, subscribers' preferences, voluntary roles, governance, donations, application decisions and necessary accounting or fraud-prevention records. Donations and enquiry submissions must not automatically become permission for unrelated marketing or political profiling.

We do not seek to collect complete card details where a suitable payment provider can handle them. DBS and other criminal-record material must be handled under their specific rules. Access to private role, donor and case information is limited to people who genuinely need it.

9. Parent Contribution Service (PCS)

PCS is a service operated by Right First Time UK Ltd, **not a separate company**. It may process parent contact information, child-related details, agreements, messages, user-supplied payment records, safety concerns and relevant evidence in support of its service.

PCS does not itself receive, hold or transfer parent-to-parent child-contribution money or exercise statutory CMS enforcement powers under the current model. PCS access must be role-restricted; child-related and other sensitive information requires stronger protections. Its dedicated PCS privacy and records policy also applies.

10. Website cookies, analytics and direct marketing

Website logs, account sessions and security information are distinct from optional analytics. The Cookie & Storage Technologies Policy explains essential cookies, optional Google Analytics 4 and visitor controls. We must not send unnecessary private case details to analytics tools.

Marketing and campaign messages will follow applicable PECR and UK GDPR requirements. Consent or another applicable basis must be established as required; we keep opt-out/suppression records where necessary and respect unsubscribe requests.

11. Sharing, suppliers and international transfers

We share personal information only where necessary, lawful and proportionate, such as with authorised service providers, professional advisers, payment processors, safeguarding authorities, regulators, police or courts when justified. A request from an official body does not itself remove the need to check its authority, purpose and scope.

Where another organisation processes information on RFTUK's behalf, appropriate Article 28 contractual terms and security checks are required. Restricted transfers outside the UK must use a lawful transfer route, such as adequacy or suitable safeguards, with any necessary transfer-risk assessment. Where a person asks us to share a document, we should confirm the scope and protect unrelated third-party information.

12. AI, automated decisions and high-risk processing

RFTUK may use approved AI and digital tools for drafting, research organisation, accessibility and other authorised work. **Passwords, safeguarding disclosures, restricted family-court material and identifiable sensitive case files must not be submitted to external AI services without a documented assessment and authorisation.**

AI workflows involving personal information require review of purposes, lawful bases, provider roles and terms, retention, security, accuracy, human oversight and international transfers. We will undertake a Data Protection Impact Assessment (DPIA) where processing is likely to result in high risk. Any solely automated decision with legal or similarly significant effects must meet the law and applicable safeguards.

13. Security and access controls

RFTUK applies measures proportionate to risk, including account permissions, secure hosting, supported software, strong authentication, encryption where suitable, backups, confidentiality commitments, logging and access removal when roles end.

Sensitive case information should not be copied into personal email accounts or devices without authorisation and safeguards. Sharing a volunteer or Director title does not automatically give access to private records. Passwords and authentication codes must never be placed in ordinary case notes or publicly accessible channels.

14. Keeping data accurate and for no longer than needed

We will use appropriate record categories and retention rules that take account of the stated purpose, accounting and other legal requirements, safeguarding, complaints, limitation periods and evidential needs. Data should not be retained indefinitely merely because digital storage is inexpensive.

Records should be corrected where inaccurate and securely deleted, destroyed or appropriately anonymised when no longer required. Sometimes a disputed historical record must be preserved with a correction note rather than silently overwritten.

15. Your data protection rights

Depending on the purpose, basis and circumstances, an individual may have rights to be informed, access, rectification, erasure, restriction, portability, objection, withdrawal of consent and safeguards connected with significant automated decisions. Rights are not absolute; lawful exemptions and the rights of others can apply.

You can contact RFTUK about your data rights using our Contact Us page. We will consider the substance of a request even when legal terminology is not used.

16. Subject access requests (SARs)

You can request access to your personal data verbally or in writing. We aim to respond without undue delay and normally **within one month**, subject to applicable rules on identification, clarification, statutory extensions and exemptions.

Replies should be secure and understandable, with reasonable protection for other people's confidential information. We do not require a person to use the expression "subject access request" before recognising the request.

17. Data protection complaints — clear route

A complaint about how RFTUK handles personal information can be submitted through our Data Protection Complaint form, our Contact Us page or by emailing complaints@rightfirsttimeuk.com. A complaint received through another ordinary RFTUK channel should still be recognised and directed appropriately.

Under the data-protection complaints rules in force since June 2026, RFTUK **must acknowledge a data protection complaint within 30 days of receipt**, investigate it appropriately without undue delay, keep the person informed as appropriate, and communicate the outcome. We aim to acknowledge ordinary complaints within five working days under our separate Complaints Policy.

People can also contact the Information Commissioner's Office (ICO) where appropriate; making a complaint to RFTUK does not remove their statutory rights.

18. Personal data breaches

A suspected personal data breach must be reported internally and assessed promptly so RFTUK can contain the incident, preserve necessary evidence and decide on legal notification obligations.

When required by the UK GDPR, the ICO must be notified without undue delay and, where feasible, **within 72 hours** of awareness. Individuals must also be informed without undue delay where the breach is likely to result in a high risk to their rights and freedoms. We keep an appropriate internal incident record, including where no ICO notification is required.

19. Publishing evidence, anonymisation and requests from authorities

Case studies, campaign material and reports should use only the information necessary to make the point. Removing a name may not anonymise a person if other details can identify them; redaction and contextual risk review are essential.

Requests for records from police, courts or public authorities must be checked for authority, necessity and proportionality. Information may be disclosed when lawfully required or justified, but RFTUK should not disclose entire files where narrower information is sufficient.

20. Training, accountability and audit records

Directors, staff, Campaign Leaders, Volunteers, contractors and others with authorised access must follow role-appropriate security and confidentiality requirements. RFTUK should provide proportionate training and review access routinely.

Governance records may include processing inventories, lawful-basis assessments, DPIAs, processor terms, data-sharing and transfer decisions, rights-request logs, breach records and retention schedules where appropriate. Personal information in internal records remains subject to confidentiality and retention controls.

21. Official guidance and related policies

This policy should be read with the RFTUK policy library, including our Privacy Notice, Cookie & Storage Technologies Policy, Information Security arrangements, Safeguarding Policy, Complaints Policy, Evidence and Corrections Policy, AI governance procedures, and the dedicated PCS privacy policy.

Independent official guidance: ICO lawful bases; ICO data-protection complaints; ICO subject access; ICO data-protection fee.

22. Review and company information

This policy will be reviewed at least annually and sooner where RFTUK services, safeguarding risks, data-protection law, ICO guidance, security processes or technologies materially change. The previous policy date was **16 June 2026**; the latest revised version is dated **12 October 2026**.

Right First Time UK Ltd — Company number **17493370** — Private company limited by guarantee, operating on a non-profit basis — rightfirsttimeuk.com. Governance and authorised volunteer roles are ordinarily unpaid at this stage, subject to authorised expenses; any future paid position requires proper approval and compliance with the company's Articles and applicable law.