

RIGHT FIRST TIME UK LTD

Privacy Notice

Privacy. Dignity. Security. Accountability.

Last updated: 13 October 2026 | Review: at least annually and after significant data-use changes

Legal controller: Right First Time UK Ltd | Company No. 17493370

Registered office: 82A James Carter Road, Mildenhall, IP28 7DE, England

Incorporation accepted: 3 October 2026

We collect and keep only the information reasonably needed. Supplying a document does not automatically give us permission to retain, share or publish every detail.

1. About this notice and who is responsible

This notice explains how Right First Time UK (RFTUK) collects, uses, stores, shares and protects personal information when people use our websites or services; contact us; volunteer, campaign, subscribe, join Public Membership or donate; attend events; make complaints; or provide evidence. It is the public-facing companion to our Data Protection & GDPR Policy.

For processing that we determine and carry out in our own right, the controller is Right First Time UK Ltd, a non-profit company limited by guarantee (Company No. 17493370). The company's incorporation was accepted on 3 October 2026. Its registered office is 82A James Carter Road, Mildenhall, IP28 7DE, England. Other organisations may be separate or joint controllers for their own processing.

2. Contacting us about your information

For privacy questions, data-protection rights requests, concerns about a possible personal data breach or a data-protection complaint, contact us using <https://rightfirsttimeuk.com/contact-us.php>. You can also email complaints@rightfirsttimeuk.com about a data-protection complaint. Please say that your enquiry concerns personal information so it reaches the appropriate team.

You do not need to contact an individual Director privately. You may also complain to the Information Commissioner's Office (ICO); see the external guidance at the end of this notice.

3. Information we may collect

The categories depend on how you engage with us. We collect information only where there is an identified and lawful purpose.

- Names, contact details, communications, enquiries and requests for support or signposting.
- Campaign, petition, consultation, subscription, Public Membership and participation records.
- Volunteer, Campaigner, Campaign Leader, Director and other governance or application records.
- Donations, payments, transaction references, refunds, event attendance and accessibility requests.
- Complaints, relevant evidence, safeguarding material and documents people choose to provide.
- Lawfully collected photographs, recordings, website access logs, device information and security events.

4. Please share only what is needed

Some enquiries concern medical information, disability, benefits, finances or court proceedings. Please do not send passwords, full payment-card numbers, complete court bundles, copies of identification or unrelated third-party details unless specifically needed. A short summary or suitably redacted document is often safer.

Receiving a document does not mean RFTUK needs to keep, circulate or publish every part. We may ask for a smaller extract, remove unnecessary information or decline to retain material that is not relevant.

5. Why we use personal information

We may use information to answer enquiries; provide guidance or signposting; operate campaigns, petitions and events; run Public Membership and communications; administer Volunteers, Campaign Leaders and company governance; process donations, payments and refunds; investigate complaints or misuse; meet accounting and legal duties; protect people from harm; secure our systems; and evaluate or improve accessibility and services.

Public-interest research may use anonymised or appropriately de-identified information. We will assess any proposed publication separately, especially where people or families could be identified.

6. Lawful bases for processing

We identify an appropriate Article 6 UK GDPR lawful basis for each activity. Depending on the facts, this may be consent, contract or requested pre-contract steps, legal obligation, vital interests, legitimate interests (following the required balancing assessment), or recognised legitimate interests where its statutory conditions apply. Public task is used only where there is a proper basis in law.

A campaign, safeguarding purpose or general claim of public interest does not automatically provide its own lawful basis. Where we rely on legitimate interests, we consider necessity, reasonable expectations and the individual's rights, including relevant objection rights.

7. Consent and your choices

Where consent is our lawful basis, it must be a genuine, informed choice. You can withdraw it without making earlier lawful processing unlawful. We will stop processing based only on that consent unless a separate legal basis properly applies.

Where a positive consent choice is legally required, we do not treat pre-ticked boxes, silence or continued browsing as permission.

8. Sensitive information and criminal allegations

Information concerning health, disability, ethnicity, religion, political opinions, trade-union membership, sex life or sexual orientation may be special-category data. In addition to an Article 6 lawful basis, we must identify a relevant Article 9 condition and meet any additional Data Protection Act 2018 requirements.

Allegations, convictions and other criminal-offence data require additional legal safeguards and an appropriate statutory condition or authority. We restrict access, distinguish allegations from findings, and do not treat information someone sends us as automatically verified.

9. Safeguarding, children and family courts

We take particular care with children's personal information, adults at risk and sensitive safeguarding disclosures. We assess what information is necessary and who needs to see it. Where lawful sharing is needed to protect someone from serious harm or make a safeguarding referral, complete confidentiality cannot be promised.

Information supplied by a parent or another person about a child is not automatically suitable for retention or publication. Family-court papers may be subject to statutory restrictions, reporting restrictions or court orders. We may ask for a redacted summary and will not treat possession as permission to publish.

10. Complaints, research and campaign evidence

For a complaint, case enquiry or campaign submission we may keep relevant correspondence, findings, decisions, supporting evidence and an audit trail. This may include information about other people, whose privacy also matters. We review whether each part is necessary and whether it can be minimised, redacted or anonymised.

Data used in published research, reports, case studies, media and public campaigns requires an additional review of accuracy, privacy, safeguarding, confidentiality and any applicable legal restrictions.

11. Volunteers, campaigners and governance

We may process application forms, contact information, roles, appropriate training, access permissions, authorised expenses, conflicts of interest and relevant safeguarding or DBS information where lawful. Access is limited by role and need.

An individual's lawful political involvement does not automatically justify unnecessary profiling. Relevant potential conflicts may be documented where necessary to protect RFTUK's political independence and governance.

12. Public Membership, subscribers and PCS

Public Membership and subscriber administration may involve contact details, payment or access status, preferences and service records. Public Members are not automatically statutory company Members or guarantors. We keep unsubscribe preferences and necessary suppression records so that people who opt out are not wrongly contacted again.

Parent Contribution Service (PCS) is operated by Right First Time UK Ltd, not by a separate company merely because it has its own service name. The dedicated PCS privacy information must also explain parent and child data in accounts, agreements, messages, records, evidence uploads and safety arrangements. PCS does not itself receive, hold or transfer parent-to-parent maintenance money or exercise statutory enforcement powers.

13. Donations and other payments

Where relevant we may keep payer identity, contact details, amounts, dates, transaction references, refunds, chargebacks and accounting records. Appropriate payment providers normally handle full card details; RFTUK should not collect or store complete card information unnecessarily.

RFTUK is not a registered charity and does not offer Gift Aid for ordinary RFTUK donations. The fee paid to RFTUK for PCS access is distinct from any voluntary parent-to-parent contribution.

14. Marketing, fundraising and campaign messages

Email, text and similar communications promoting campaigns, fundraising, Public Membership or organisational aims may be direct marketing. We apply the relevant UK GDPR and PECR requirements, seek consent where required and provide a clear opt-out or unsubscribe mechanism.

An enquiry, complaint, petition signature, donation or website visit does not automatically authorise later marketing. We do not rely on a charity-specific electronic-mail soft opt-in where RFTUK does not meet its conditions.

15. Websites, security logs, cookies and analytics

Our sites may process IP addresses, device and browser details, timestamps, login and security events and diagnostic records to deliver services, protect accounts, detect misuse and investigate faults. We limit access and retention according to the purpose.

Essential storage may support login, preferences and security. Optional analytics, including Google Analytics 4 where enabled, may set cookies such as `_ga` and `_ga_*` only in accordance with the applicable consent rules. Our Cookie & Storage Technologies Policy and Website Analytics Policy explain how to accept, reject or change preferences. Continued browsing is not consent where a positive choice is required.

16. AI and digital service providers

Approved AI and digital tools may assist with drafting, coding, translation, accessibility, research organisation or media work. We do not treat external AI systems as unrestricted repositories for personal cases or confidential files.

Before sharing personal information with a provider, we consider necessity, data minimisation, lawful basis, terms, security, retention, any restricted international transfer and human oversight, including whether a Data Protection Impact Assessment is required. Passwords or unnecessary identifying safeguarding information must not be uploaded without specific assessment and authorisation.

17. When information may be shared

Where lawful and necessary we may disclose information to hosting, email, payment or IT suppliers; accountants, auditors and legal advisers; authorised contractors; safeguarding services; police; courts; regulators; public authorities; or an MP or relevant organisation where you ask us to make an appropriate referral.

Sharing is limited to what the particular purpose requires, with appropriate confidentiality or legal safeguards. We do not sell personal information. No partner or sponsor automatically receives access to confidential member, complaint, safeguarding or PCS records.

18. Processors and international transfers

Where a supplier processes personal information on our instructions, we use appropriate controller-processor terms and security arrangements as required by law. Other organisations may instead act as separate or joint controllers; their responsibilities must be assessed on the facts.

Cloud, email, analytics, payment or AI services may involve processing outside the UK. Where a restricted international transfer occurs, we must use an appropriate legal route, including adequacy regulations or valid transfer safeguards where required. Transfer compliance does not replace the need for a lawful basis and security.

19. Security and confidentiality

RFTUK aims to protect personal information with proportionate technical and organisational controls, including appropriate account permissions, restricted access, secure systems, logging, supplier checks, backup and incident-response arrangements.

We do not promise that any internet-based service is absolutely risk-free. Confidential information should be available only to those with an authorised purpose, and disclosure for publicity is not automatic simply because information was sent to RFTUK.

20. How long records are kept

We keep personal data only as long as justified by the purpose and applicable legal, accounting, complaint, safeguarding or evidence needs. Typical approaches include routine enquiries for normally up to 12 months after closure unless an exception applies; subscriber details while subscribed plus proportionate suppression records; member and role records for the relevant period plus lawful follow-up; and core tax or financial records for the legally necessary period (often six years or longer where required).

Serious legal, safeguarding or complaint files may need justified longer retention; website security logs should not be kept indefinitely by default. Our Records Retention & Destruction Policy provides more specific rules. Where no longer required, records should be safely deleted, destroyed or irreversibly anonymised.

21. Your data-protection rights

Depending on the activity and any legal exemptions, you may have rights to information, access, correction, erasure, restriction, portability, objection, withdrawal of consent and safeguards concerning significant automated decisions. Not all rights apply to every kind of processing.

Contact us if you believe information we hold is inaccurate or you wish to exercise a right. We will explain any applicable exception, request for identity verification or other lawful limitation.

22. Subject access requests

You can ask verbally or in writing for access to your personal information. We will respond without undue delay and normally within one month under the applicable UK GDPR rules, subject to lawful clarification, identity checks, extensions or exemptions.

Records may contain information about others. We consider those people's rights before releasing information and will not disclose third-party material unlawfully.

23. Data-protection complaints and breaches

If you think we have mishandled your information, use <https://rightfirsttimeuk.com/contact-us.php> or complaints@rightfirsttimeuk.com. Under the data-protection complaint requirements in force since June 2026, we will acknowledge a qualifying complaint within 30 days, investigate it appropriately and inform you of the outcome. You may complain to the ICO without losing that right by contacting RFTUK first.

If a personal data breach occurs, we assess and contain the incident. Where reportable, we notify the ICO without undue delay and, where feasible, within 72 hours of awareness. Where legally required because the risk to affected individuals is high, we will also notify them without undue delay.

24. Information from others and automated decisions

We may receive relevant information from public records, complainants, representatives, authorities, professional advisers or campaign sources. We consider its reliability and provide privacy information where the law requires, unless an applicable exemption applies.

RFTUK does not currently intend to use solely automated decision-making that produces legal or similarly significant effects. If that changes, we will update this notice and provide the safeguards required by the law in force.

25. Keeping this notice up to date

We review this notice at least annually and earlier if important laws, services, suppliers or data uses change. A materially new use may require additional notice or another assessment before it begins. This notice does not replace any service-specific terms or the dedicated PCS privacy information.

Related policies include Data Protection & GDPR, Cookie & Storage Technologies, Website Analytics, Information Security & Cybersecurity, Safeguarding, Complaints, Volunteer, Evidence & Corrections, Donation Transparency, and AI Images & Visual Content. They are available in the RFTUK policy library.

Related information and official guidance

[Contact Us / privacy requests](#)

[Data Protection & GDPR Policy](#)

[Cookie & Storage Technologies Policy](#)

[Policy library](#)

[ICO - Your right to be informed](#)

[ICO - Data protection complaints](#)

[ICO - International transfers](#)

Right First Time UK Ltd is a private company limited by guarantee operating on a non-profit/public-benefit basis. PCS is a service of the company and not a separate legal entity merely because it uses the PCS name.