

Risk Management Policy

Identify Early. Own Clearly. Control Proportionately.

Right First Time UK Ltd · Company number 17493370 · Incorporation accepted 3 October 2026

Registered office: 82A James Carter Road, Mildenhall, IP28 7DE, England. Updated: 13 October 2026. Review at least annually and after material change.

At a glance: 5 × 5 scoring · named owners · immediate critical-risk escalation · safeguarding and legal duties always take priority.

1. Purpose and scope

This policy explains how Right First Time UK (RFTUK) identifies, assesses, records, manages, escalates and reviews risks affecting its people, activities, finances, public-interest campaigns, systems, legal duties, reputation and continuity.

It applies to Directors, officers, Campaign Leaders, Volunteers, contractors and any person authorised to manage an RFTUK activity or material risk. It covers public membership, fundraising, publications, events and the Parent Contribution Service (PCS).

2. Governance, accountability and the registered Articles

Right First Time UK Ltd is a registered private company limited by guarantee (Company No. 17493370; incorporation accepted 3 October 2026). Directors retain governance oversight and must act within their legal duties and the registered Articles of Association. Founder rights, reserved matters and any applicable approval requirements under the Articles must be respected; this policy cannot amend them.

Responsibility for day-to-day controls may be delegated, but Directors should understand principal risks, consider adequate resources and receive timely reports. Risk ownership must be clear and consistent with actual delegated authority.

3. Risk culture, appetite and tolerance

People should raise concerns early and respectfully, even when the information is unwelcome. RFTUK seeks evidence, accountable decisions, proportional controls and learning from mistakes without penalising honest reporting.

Risk appetite may be higher for reversible innovation and campaigning than for safeguarding, privacy, fraud, solvency, legal compliance or serious safety matters. Risk tolerance is the boundary at which extra controls or senior approval become necessary. Neither appetite nor a numerical score permits unlawful conduct or disregard of urgent harm.

4. Risk categories and principal risks

- Governance, legal duties, company decision-making and political or electoral compliance
- Financial viability, fraud, donation restrictions, fundraising, payments and procurement
- Children and adults at risk, safeguarding, health and safety, events and lone working
- Privacy, data breaches, cybersecurity, AI tools, website/email continuity and suppliers
- Evidence quality, defamation, family-court restrictions, media and reputational impacts
- Volunteers, capacity, accessibility, conflicts of interest and partnerships
- Public Membership and PCS operations, communications, calculations and records

A principal risk is one capable of materially threatening RFTUK objectives, continuity, legal position or people. Such risks must be visible to the Directors.

5. Identify and describe risks

Identify risks during planning, procurement, complaints, safeguarding referrals, system changes, financial reviews, audits, incidents, near misses and emerging legal or technological developments. Consider what could happen, why, who might be affected and the credible consequences. Do not use vague labels without a cause or impact.

6. Risk register and named responsibility

RFTUK should maintain a live register of material risks, with a named risk owner and separate action owner where appropriate. Every material treatment action should have a realistic deadline. Sensitive security, safeguarding and legal details should be kept in a restricted annex rather than widely distributed.

Use Appendix B as the minimum practical register template. Overdue or unowned high risks must be escalated, not left open without a decision.

7. Inherent and residual assessment

Inherent risk is assessed before existing controls; residual risk is assessed after the controls that actually operate. Planned, untested or non-functioning measures must not be counted as effective. Reassess when conditions, threats or controls change.

8. Likelihood scale (1-5)

- 1 — Rare: exceptional circumstances
- 2 — Unlikely: conceivable but not expected
- 3 — Possible: realistic chance within the relevant period
- 4 — Likely: expected to occur or recur
- 5 — Almost certain: expected frequently or in most relevant circumstances

Use a sensible timeframe. A likelihood score is an informed judgement, not a precise probability.

9. Impact scale (1-5)

- 1 — Insignificant: minimal loss or disruption
- 2 — Minor: limited impact managed in ordinary operations
- 3 — Moderate: meaningful financial, legal, service or reputational effect
- 4 — Major: serious harm, significant loss, substantial interruption or legal exposure
- 5 — Severe / critical: risk to life, severe safeguarding harm, existential loss, serious legal consequences or prolonged critical-service failure

Use the most credible significant consequence, recognising that different people can experience harm differently.

10. Scoring and risk bands

Score = likelihood × impact (range 1–25). RFTUK uses: Low 1–4; Moderate 5–9; High 10–16; Critical 17–25. The full 5×5 matrix is in Appendix A. The bands guide priorities; credible immediate danger or a legal duty overrides the calculated band.

11. Escalation and review frequency

- Critical (17–25): escalate immediately to senior leadership/Directors; take immediate containment action and review frequently. Use emergency or statutory routes when required.
- High (10–16): prompt treatment, named owner and Director visibility for material issues; normally review actions at least monthly.
- Moderate (5–9): active management and proportionate review, normally at least quarterly while material.
- Low (1–4): routine controls and periodic review; escalate if circumstances deteriorate.

Escalate regardless of score where authority or tolerance is exceeded, risks affect several functions, or urgent harm, insolvency, safeguarding, fraud or legal breach may occur.

12. Treatment, acceptance and authorisation

Appropriate responses include stopping or avoiding an activity, reducing likelihood or impact, sharing some consequences through insurance/contract, or accepting residual risk within approved authority. Insurance and outsourcing do not remove RFTUK responsibilities.

A risk owner must not accept risk beyond their powers. Critical residual risk should not normally be accepted without Director-level consideration and relevant legal/specialist advice. Record who decided, why, and when to reconsider.

13. Controls, testing and assurance

Controls can be preventive, detective, corrective or recovery-based: spending approvals, separation of duties, MFA, access reviews, backups, safeguarding referrals, incident procedures, conflict declarations, fact-checking and supplier checks.

Assess whether controls exist, are understood, are used and are tested. Evidence may include reconciliations, system logs, restored backups, training records, incident analysis, independent checks and documented approvals; reassurance alone is not assurance.

14. Safeguarding and immediate safety

RFTUK has low tolerance for safeguarding risk. A credible urgent threat to a child or adult at risk calls for timely protective action and suitable external referral; completing a risk-score form must never delay emergency response. Record sensitive details with restricted access under the Safeguarding Policy.

Events, travel and lone working also require activity-specific assessments when appropriate; a general risk-register entry does not substitute for legally required health-and-safety assessment.

15. Financial integrity, fraud and solvency

Monitor cash flow, liabilities, recurring subscriptions, donor restrictions, fraud, misuse of funds and payment-provider exposure. Spending must be authorised under financial controls and consistent with the registered Articles. Potential insolvency requires timely Director consideration of legal duties and creditor interests.

Suspected fraud or bribery may require immediate access restrictions, preservation of evidence, independent review and, where appropriate, external reporting.

16. Privacy, cybersecurity and digital systems

Risks from personal data, databases, email, Plesk/hosting, domain recovery, AI services, online forms and payment systems must have accountable owners and proportionate technical controls. Where required, a separate Data Protection Impact Assessment (DPIA) must be completed; a risk-register score alone is insufficient.

Assess security incidents promptly, preserve evidence, consider breach-reporting duties, monitor supplier access and test recovery procedures. Do not publish specific vulnerabilities or credentials in the public risk register.

17. Suppliers, partnerships and business continuity

Assess critical suppliers for failure, price increases, security compromise, data lock-in, contract termination and business continuity. Keep recoverable organisational control of websites, domains, email, backups and payment-related services. Use supplier due diligence and appropriate written contracts.

Contingency planning should identify which services and records need restoring first, who has recovery access and how the public can reach RFTUK during an outage.

18. Publications, campaigning and legal risks

Before high-risk publication or campaigning, consider accuracy, evidence, privacy, defamation, right of reply, court restrictions, safeguarding, digital imprints and relevant electoral obligations. RFTUK remains non-party political; risk review supports lawful public-interest criticism rather than concealing wrongdoing.

Keep suitable approval, correction and version records; reassess campaigns when public circumstances or regulatory periods change.

19. People, capacity and organisational changes

Assess the effect of unfilled roles, volunteer capacity, fatigue, inaccessible processes, incomplete training, key-person dependence and account access remaining after people leave. Significant changes—new memberships, services, fundraising, events, campaigns, software, AI or payment arrangements—should receive proportionate risk review before launch.

Opportunity should be weighed alongside risk. Controls must allow responsible development and participation, not create unnecessary bureaucracy.

20. Parent Contribution Service (PCS)

PCS is a service of Right First Time UK Ltd, not a separate legal entity. It provides voluntary parent-to-parent information, calculation, communication, agreements and records; it is not CMS and has no statutory enforcement powers. Under the current model, RFTUK does not receive, hold or transfer parent-to-parent child-contribution funds; PCS service-access fees paid to RFTUK are separate.

PCS assessments should cover inaccurate calculations or representations, coercion/domestic abuse, unsafe communication, disputed logs, child data, privacy/security breaches, unauthorised access, outages, payment-regulation boundaries and service-provider failures. Escalate material safeguarding or legal risks promptly.

21. Incidents, near misses, reporting and review

Actual incidents and near misses should inform risk scores and improvements. Record what happened, what controls worked, what assumptions failed, the action owner and due date. Directors should review principal risks at suitable intervals; the organisation-wide register receives a formal review at least annually and after material incidents.

Reports should highlight new or worsening risks, overdue actions, significant losses, incident trends, risk decisions and whether controls are effective—not bury important matters in low-value detail.

22. Records, confidentiality and contact

Keep risk registers, assessments, control tests, approvals, escalations and significant incidents under the Records Retention & Destruction Policy, including applicable legal holds. Publish high-level themes where useful, without revealing confidential safeguarding identities, cyber weaknesses, legal advice or whistleblower information.

Questions, concerns or risk-escalation requests can be sent through the Contact Us page or complaints@rightfirsttimeuk.com. Emergency risks require the appropriate emergency, safeguarding or statutory route. Review this policy at least annually and after substantial changes.

Appendix A — 5 × 5 risk-scoring matrix

Likelihood (1–5) across; impact (5–1) down. Score = likelihood × impact. Bands: Low 1–4; Moderate 5–9; High 10–16; Critical 17–25.

Impact / likelihood	1	2	3	4	5
5	5 — Moderate	10 — High	15 — High	20 — Critical	25 — Critical
4	4 — Low	8 — Moderate	12 — High	16 — High	20 — Critical
3	3 — Low	6 — Moderate	9 — Moderate	12 — High	15 — High
2	2 — Low	4 — Low	6 — Moderate	8 — Moderate	10 — High
1	1 — Low	2 — Low	3 — Low	4 — Low	5 — Moderate

Appendix B — risk register fields

Field	Purpose
Risk ID / title / category	Unique reference and risk type
Cause / event / consequence	What could happen and the resulting harm
Existing controls	Controls currently implemented and evidenced
Inherent likelihood / impact / score	Exposure before operating controls
Risk owner	Accountable person
Further action / action owner / deadline	Treatment and delivery responsibility
Residual likelihood / impact / score	Exposure after operating controls
Status / next review	Progress and review date
Decision / escalation / approval	Who accepted or escalated risk and why

Related RFTUK policies

- [Governance & Transparency](#)
- [Financial Controls & Expenses](#)
- [Safeguarding](#)
- [Data Protection & GDPR](#)
- [Information Security & Cybersecurity](#)
- [Procurement & Supplier](#)
- [Records Retention & Destruction](#)
- [Evidence, Research & Corrections](#)
- [Health & Safety / Lone Working](#)
- [Registered Articles of Association](#)

Official guidance

- [HM Treasury Orange Book \(voluntary benchmark\)](#)
- [GOV.UK: Directors general duties](#)
- [NCSC: Cyber Governance Code of Practice](#)
- [HSE: Risk assessment](#)

External resources are background guidance; a voluntary benchmark is not automatically mandatory for RFTUK.

Company, voluntary status and PCS alignment

Right First Time UK Ltd is a private company limited by guarantee (17493370). Its registered Articles control statutory company powers, approvals and governance. Genuine authorised expenses and any later paid role remain subject to the Articles and applicable law. PCS is a voluntary service run by RFTUK and not a separate legal entity or statutory maintenance authority.

Contact: rightfirsttimeuk.com/contact-us.php · complaints@rightfirsttimeuk.com