

PROCUREMENT & SUPPLIER POLICY

Buy Carefully. Contract Clearly. Review Regularly.

Right First Time UK Ltd | Company No. 17493370 | Accepted 3 October 2026
Policy updated: 13 October 2026 | Review: at least annually or after material changes

Buy what RFTUK genuinely needs, at a reasonable total cost, from a supplier suitable for the risk.

1. Purpose and scope

Right First Time UK Ltd (RFTUK) uses this policy to select, authorise, contract with, monitor and, where appropriate, replace suppliers. It covers goods, subscriptions, hosting, domain services, software and AI, contractors, professional advice, events, printing, travel, advertising, payment and fundraising services.

The policy applies to Directors, authorised staff, Campaign Leaders, Volunteers and contractors involved in purchasing or supplier management. Our registered Articles of Association and lawful delegated powers take precedence over this operational policy.

2. Basic purchasing principles

Purchasing must be lawful, proportionate, recorded where material, free from improper influence, secure, accessible where appropriate and demonstrably connected with RFTUK's objectives. Value for money considers total lifetime cost, quality, service continuity, support, safety, security and usability—not price alone.

RFTUK is not automatically a public authority under public-procurement legislation. We use good-governance principles without claiming public-sector procurement duties automatically apply.

3. Director accountability and authority

Directors remain accountable for proper company governance, informed judgement and conflict management, even when supplier work is delegated. Commitments must follow the registered Articles, relevant Founder/Member approval protections where applicable, and the Financial Controls & Expenses Policy.

An approved Financial Authority Schedule or equivalent written record should identify who can authorise purchasing and the relevant monetary, duration and contract limits. This policy does not create monetary authorisation limits. Campaign Leaders and Volunteers do not acquire power to bind RFTUK merely through their role.

4. Justifying a purchase

Before a material commitment, document what is required, the reason, available alternatives, expected total cost, contract period, source of funds and whether an existing tool or service already meets the need. Respect restrictions attached to grants and donations.

Consider running costs, VAT, transaction fees, price increases, add-ons, data export, cancellation charges, equipment and support as well as the initial quoted price.

5. Competition and single-supplier selection

Compare proportionate alternatives using quotations, published prices or documented market checks when practical. Routine inexpensive purchasing need not involve formal tenders.

Where one supplier is chosen for urgency, special expertise, compatibility, intellectual-property restrictions or genuine lack of alternatives, record the reason for material purchases. Personal familiarity alone is not sufficient justification.

6. Risk-based supplier checks

Assess suppliers according to potential impact. Low-risk routine purchases need simple checks; higher-risk arrangements require more detailed examination of identity, terms, financial resilience, professional or regulatory status, insurance where relevant, security, privacy, ethics and safeguarding.

Higher-risk examples include organisations handling sensitive personal or safeguarding data, payment access, website/domain administration, confidential research, major recurring expenditure, vulnerable people or public-facing RFTUK representation. Do not request irrelevant personal or corporate paperwork.

7. Connected suppliers and conflicts

Personal, family, financial, professional or other material connections to a supplier must be declared before the decision. A connected supplier is not automatically excluded, but must offer reasonable terms, serve RFTUK's interests and be considered under the Articles and Conflict of Interest Policy.

An interested person must not improperly choose the supplier, approve their own arrangement and authorise payment without appropriate independent safeguards. Supplier gifts, secret commissions and improper hospitality are prohibited under the Gifts, Hospitality & Anti-Bribery Policy.

8. Hosting, domains and critical technology

Domain names, DNS, web hosting, email, databases, code repositories, payment platforms and administrator accounts require special continuity planning. RFTUK should retain organisational ownership or appropriate contractual control, account-recovery routes, secure backups and access to source files and data.

Contractors must not be the only people able to recover an essential account, domain or database. Assess authentication, incident reporting, subcontractors, support, recovery testing, export procedures and replacement options; use relevant NCSC guidance for complex or high-risk contracts.

9. Data protection and international processing

Determine whether a provider is a processor, independent controller or another type of recipient. Where Article 28 UK GDPR applies, use a compliant written agreement addressing instructions, confidentiality, security, subprocessors, assistance with rights and breaches, and return or deletion of data.

Assess restricted international transfers separately and use an appropriate legal mechanism when required. Marketing claims of "GDPR compliant" do not replace examination of the supplier's actual arrangements. Minimise access to sensitive case data.

10. Payments, fundraising and professional suppliers

For payment processors and fundraising platforms, assess fees, settlement recipient, account security, refund and dispute procedures, fraud protection, information handling and exit terms. Confirm who receives money and when.

For lawyers, accountants and other specialists, check credentials and regulatory authorisation where relevant, scope, fees, conflicts and adequate evidence of work. Contractor arrangements should include genuine employment-status assessment where needed.

11. Ethical supply, inclusion and independence

Consider the Modern Slavery & Ethical Supply Policy for labour-intensive, subcontracted or opaque services and products, including branded merchandise. Avoid unsupported assertions that any supply chain is entirely exploitation-free.

Choose suppliers fairly: do not reward or penalise lawful party-political affiliation, apply unlawful discrimination or disregard relevant accessibility and reasonable-adjustment needs. Environmental or local-benefit claims should be evidence-based rather than a cover for favouritism.

12. Contracts and written approvals

A person with suitable delegated authority must review material terms before signing, clicking "accept" or starting a recurring subscription. Important terms include the parties, work scope, performance standards, total price, payment schedule, data handling, confidentiality, intellectual property, duration, liability, renewal, cancellation, dispute handling and exit.

Where appropriate, keep written approval or a purchase order showing supplier, proposed spend, budget and approver before work begins. Escalate unusually high-risk or complex contracts for suitable professional review.

13. Recurring charges and renewals

Keep a record of subscription owner, purpose, fee, billing interval, renewal and notice dates and how to cancel. Review unused, duplicated or poor-value services periodically.

Free trials can become paid contracts. Record the trial end date and any automatic-renewal notice period before activating the service.

14. Invoices, bank details and restricted funds

Compare invoices with authorised prices, delivered work and supporting evidence. Query duplicate or unexpected charges before payment. Independently verify significant changes of supplier bank details where fraud is a concern.

Restricted grants or donations may only be used consistently with their relevant terms. Accounting and payment records must follow Financial Controls & Expenses procedures; no supplier can override those controls.

15. Supplier performance and incident response

Proportionately review material contracts for cost, service quality, security, privacy, accessibility, reliability and complaints. Record failures and seek correction, refunds, service credits or other contractual remedies as appropriate.

Escalate cybersecurity incidents immediately under the Information Security & Cybersecurity Policy. Investigate affected systems and data, assess personal-data breach obligations, safeguard evidence and consider supplier response when deciding whether to renew.

16. Supplier disputes and emergency purchasing

Handle commercial disputes professionally, preserve material records and distinguish ordinary performance failures from fraud, cyber incidents, safeguarding problems or other serious concerns needing separate action.

Urgent safety or operational risk may justify accelerated selection, but the reason, expected cost, authority and supplier choice should still be recorded as soon as practicable. Avoid using repeated poor planning to bypass controls.

17. Supplier records and register

Maintain proportionate records for material or recurring providers: checks, bids, approvals, contract, conflict declarations, invoices, incidents, renewal dates and performance reviews. Store these securely in line with retention policies.

A supplier register should identify contract owner, supplier and service, recurring costs, renewal dates, risk category, data-processing status, system access, conflicts and next review. Keep safeguards proportionate for small and local suppliers.

18. Exit, continuity and intellectual property

Before and during a critical relationship, plan how to recover data, source code, records, configurations, domain control, credentials and licences on exit. Agreements should identify ownership and permitted use of deliverables and appropriate data-return or deletion arrangements.

When ending a contract, obey its termination terms, recover RFTUK property, revoke unnecessary access and confirm relevant deletion or return of personal data. Avoid any gap in control of domains, website, email, payment or other essential systems.

19. PCS-specific safeguards

The Parent Contribution Service (PCS) is operated by Right First Time UK Ltd; it is not a separate company. PCS suppliers handling parent/child data, messages, document storage, accounts or payment of RFTUK service fees must be treated as higher-risk where appropriate.

Under the present PCS model, parent-to-parent contributions are paid directly between parents, not received, held or transferred by PCS. No supplier may reroute those contributions through RFTUK without separate lawful

regulatory assessment and formal authorisation. PCS service-access fees are distinct from those contributions.

20. Governance, contact and review

This policy is supported by the registered Articles of Association and related Financial Controls, Conflicts, Gifts & Anti-Bribery, Data Protection, Cybersecurity, Modern Slavery, Safeguarding and Records Retention policies. No provision here changes company membership, Director powers or Founder rights established in the Articles.

It will be reviewed at least annually and sooner if material changes arise in suppliers, spending, cyber risks, legislation or RFTUK operations. Questions, supplier concerns or complaints can be raised through the Contact Us page or complaints inbox; emergencies should use appropriate emergency services.

Appendix A — Practical supplier approval checklist

For material or higher-risk suppliers, record what is relevant. This checklist supports proportionate decisions; it is not a guarantee.

1. Supplier and legal/trading identity; service and reason for purchase
2. Contract owner, approving authority and any conflict declaration
3. Risk level; access to personal data, systems, payment tools or vulnerable people
4. Quotations or single-supplier reason, total cost, funding source and VAT/fees
5. Data processor/controller status, written contract and any transfer assessment
6. Security controls, administrator access, backup and breach-notification procedure
7. Key contract clauses, deliverables, intellectual property and liability
8. Start date, billing cycle, renewal deadline and cancellation instructions
9. Exit/data-export route, access removal and continuity plan
10. Performance, incidents, corrective actions and next review date

Official guidance

- [GOV.UK – Directors’ duties](#)
- [ICO – Controller and processor contracts](#)
- [NCSC – Supply-chain cybersecurity](#)
- [NCSC – Cyber Essentials supply-chain playbook](#)
- [GOV.UK – Modern slavery supply-chain transparency](#)

Contact and legal identity

Right First Time UK Ltd is a private company limited by guarantee. Registered office: 82A James Carter Road, Mildenhall, IP28 7DE, England. Company No. 17493370. These standards do not amend the company’s registered Articles of Association.

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