

Information Security & Cybersecurity Policy

Protect Access. Protect Data. Protect Continuity.

Right First Time UK Ltd | Company No. 17493370 | Version 1.1 | Updated 12 October 2026

Access is granted because a role needs it—not because of title or seniority. This document sets organisational standards; it does not certify implementation of every technical safeguard.

1. Purpose and coverage

Right First Time UK Ltd (RFTUK) safeguards its websites, domains, servers, email, devices, membership systems, campaign information, payment administration and digital records against loss, misuse, unauthorised access and disruption. Cybersecurity is a governance responsibility as well as a technical function.

This policy applies to Directors, Campaign Leaders, Campaigners, Volunteers, employees, contractors and other authorised users. It covers RFTUK-controlled systems and information, including services supplied by third parties. The standards apply proportionately to the sensitivity of the work and to each person's role.

2. Director oversight and risk management

Directors retain oversight of cyber risk even where technical administration is delegated. RFTUK should identify critical systems, assign responsible persons, review significant risks and incidents, and check that safeguards are working rather than merely documented.

Risk reviews should consider confidentiality, integrity and availability, including phishing, ransomware, financial fraud, data loss, insider misuse, supplier failure and service outages. Higher-risk decisions and exceptions should be documented and reviewed.

3. Critical systems and organisational recovery

RFTUK should maintain a secure Critical Systems Register showing each important service, its purpose, approved administrator, service provider, recovery route, authentication status, renewal date, backup dependency and data sensitivity. Priority systems include domain registration, DNS, Plesk/hosting, organisational email, banking/payment access and databases containing personal information.

Critical accounts should be controlled for the organisation where supported. Recovery must not permanently depend on one individual's private email or phone when a safer authorised route is available; equally, recovery resilience must never become unrestricted administrator access.

4. Least privilege and individual access

Access is granted because a person needs it for an authorised task—not because of their title or seniority. Campaign editors should not automatically obtain server-root, financial, safeguarding or organisation-wide database privileges. Administrator access is restricted to specifically authorised individuals.

Use individual accounts where supported. Shared credentials should be avoided; unavoidable legacy credentials must be tightly controlled, securely stored and changed when relevant personnel leave or compromise is suspected. Access should be reviewed regularly and adjusted promptly when roles change.

5. Passkeys, passwords, MFA and credential storage

Use passkeys or phishing-resistant authentication where practical. Otherwise, critical services should use strong unique passwords and multi-factor authentication (MFA). Email, domain, hosting, banking and payment accounts deserve the strongest available controls. Credentials must not be reused across critical systems.

Use an approved password or credential manager. Never place passwords, database secrets, backup codes or API tokens in public PHP files, public repositories, ordinary spreadsheets, chats or unprotected documents. Protect password-manager recovery and avoid sharing MFA codes.

6. Email, domains and hosting security

Protect organisational inboxes from account takeover, unauthorised forwarding rules, fraudulent reset messages and unknown sessions. Check unexpected security alerts and preserve current recovery information. Email compromise may also jeopardise other accounts.

Protect domain registrar and DNS access through strong authentication, limited administrators, registrar locks and change notifications where available. Plesk, VPS and root-level access must be tightly restricted; investigate firewall, Fail2Ban and login alerts rather than disabling defences to solve access problems. Record material DNS and hosting changes.

7. Website applications and software updates

Website publication permissions must be separate from system ownership, billing and server administration. Remove unnecessary plugins, integrations, abandoned accounts and unsupported components. Apply security patches promptly with suitable testing and rollback arrangements.

Production changes to authentication, payments, uploads, databases and personal data must be reviewed and tested before deployment, including AI-generated code. Maintain appropriate backups, change records and access separation.

8. Devices, remote work and personal equipment

Devices used for RFTUK work should have screen locks, supported software, updates and appropriate malware protection. Encrypt devices or storage holding sensitive data where practicable and report missing or stolen devices promptly so access can be revoked.

Personal-device use must be proportionate and authorised for sensitive information. Avoid unnecessary local copies; protect screens and conversations in public or shared spaces; use suitable network security for sensitive administration. Remove organisational data and tokens when access ends.

9. Backups, testing and continuity

Back up important website files, databases, membership records, finance data, campaign documents, source code and critical configuration. Protect backup access and keep at least one logically or physically separated recovery copy where practicable so a single compromised account cannot destroy all copies.

Test restoration at a proportionate frequency and record any failures. Recovery plans should prioritise domain/DNS, email, public website, safeguarding contact routes, payment administration and vital records. Keep authorised personnel able to reach backup and supplier details during an outage.

10. Information classification and minimisation

Handle records in practical categories: Public (approved for release), Internal (ordinary organisational information), Confidential (personal, contract, financial or unpublished material) and Highly Sensitive (safeguarding, medical details, restricted court material, bank credentials and similar high-risk data). Apply tighter access and sharing controls as sensitivity increases.

Only collect and retain information needed for a lawful purpose. Restrict special-category, criminal-offence and safeguarding information to authorised users with a genuine need; do not place it in general campaign chats or broadly shared folders.

11. Secure sharing, email and publication

Use authorised file storage and carefully scoped sharing links. Before sending an email, check addresses, recipients, attachments and whether the content needs a safer transfer method; use BCC where appropriate to protect mailing lists.

Before publishing PDFs, documents, screenshots or spreadsheets, check hidden comments, tracked changes, embedded files, metadata and personal information. Redactions must remove underlying content rather than merely cover it visually.

12. Phishing, ransomware and online fraud

Treat unexpected demands for passwords, MFA codes, urgent transfers, bank-detail changes or unusual downloads as possible scams. Verify consequential requests through an independent trusted channel, not simply by replying to the suspicious message.

Use supported systems, updates and protected backups against malware and ransomware. Isolate and escalate a suspected infection. Changes to supplier or beneficiary banking details require independent verification before significant payments are made.

13. Social media, payments and member systems

Official social-media profiles, banking, donations, membership and payment services require role-based access, suitable authentication and controlled recovery. Users who merely need to view reports must not automatically be permitted to issue refunds or alter destination accounts.

RFTUK should review providers and access permissions in proportion to the value of funds and sensitivity of data. Personal political accounts should not be the only recovery route for RFTUK social profiles where organisational alternatives are available.

14. Suppliers, contractors and external services

Consider service-provider security, data-protection arrangements, sub-processors, backups, incident contact, service continuity and exit options before granting access to sensitive systems. Contractors must receive the least access needed, preferably with individual and time-limited accounts.

RFTUK should retain organisational control of source code, domain registration, hosting recovery and critical configurations. A contractor or Volunteer must not become the sole permanent gatekeeper to RFTUK systems.

15. Secrets, API connections and AI tools

Protect source-code repositories, API keys, database credentials and secret tokens as sensitive assets; use secure server-side configuration and rotate exposed credentials. Public source files must not disclose working secrets.

Do not submit credentials, private server configurations, restricted court files or unnecessary sensitive personal information to external AI tools without specific assessment and authorisation. Check AI-assisted security advice or code before use on live systems.

16. Logging, monitoring and compromise warning signs

Keep proportionate access, system-change and security logs, with retention and access limits consistent with privacy law. Relevant events may include administrator sign-ins, failed logins, account recovery changes, DNS changes, financial actions and suspicious server activity.

Investigate unknown administrators, unexpected forwarding rules, reset emails, unexplained payments, website redirects, altered files, encrypted data or sudden account lockouts. Monitoring should protect services without unjustified surveillance of individuals.

17. Reporting and initial response

Anyone noticing suspected phishing, a lost device, unauthorised access, data loss or another cyber concern must report it promptly through an authorised internal contact. Record when it happened, affected systems and any relevant messages or screenshots without spreading malicious content.

RFTUK should assess and contain the issue, protect people, preserve evidence, revoke or rotate affected access, contact providers and restore operations safely. Serious incidents warrant suitable professional help; do not conceal an incident for reputational reasons.

18. Personal data breaches and regulatory notification

A security incident may be a personal data breach. RFTUK must assess the nature of the event, affected data and risk to individuals in accordance with the Data Protection & GDPR Policy. Where the law requires notification to the ICO, report without undue delay and, where feasible, within 72 hours after becoming aware of the notifiable breach.

High-risk breaches may also require notifying affected people. Record the facts, decisions, rationale and actions even if a breach is not reportable. Only authorised persons should communicate publicly; statements must be accurate and proportionate.

19. Incident evidence, recovery and extortion

Preserve useful logs, emails, transactions and affected files securely where lawful and safe. Do not destroy evidence simply to conceal an incident; immediate containment may nevertheless be needed to prevent harm.

Following an account takeover, use the provider's official recovery route and inspect sessions, MFA, recovery details, email-forwarding rules and linked accounts. Do not pay a ransomware or extortion demand impulsively; consider legal and law-enforcement advice, recognising that payment guarantees neither recovery nor deletion.

20. Access changes, departures and training

New participants should receive access only after authorisation and proportionate security guidance. Review access when responsibilities change; promptly remove accounts, tokens, sessions and permissions when roles end and recover organisational equipment and information.

Provide practical awareness about phishing, account recovery, secure sharing, data protection and incident reporting, especially for finance, campaign administration and website roles. Encourage prompt disclosure of mistakes rather than silence.

21. Assurance, exceptions and review

RFTUK may use NCSC guidance and consider Cyber Essentials or appropriate external testing as it grows. Certification is a useful assurance measure, not proof that every system is secure. Risk and access checks should reflect evolving systems and threats.

Any temporary security exception should specify the reason, authoriser, risks, compensating safeguards and review or expiry date. Convenience alone is not sufficient for an indefinite high-risk exception. Review this policy at least annually and after significant incidents or system changes.

22. Parent Contribution Service (PCS)

PCS is a service operated by Right First Time UK Ltd, not a separate company. Its parent accounts, agreements, messages and evidence can be highly sensitive and require role-based access, secure backups, strong authentication where available and an incident-response route.

Parent credentials must not be shared with another parent or an RFTUK Volunteer. Under the stated current service model, RFTUK does not receive, hold or transfer voluntary parent-to-parent child-contribution payments; service-access fees paid to RFTUK remain separate.

23. Complaints, related policies and contact

Information-security concerns, unsafe data sharing, suspected unauthorised access and cybersecurity incidents should be reported promptly. Use the [RFTUK Contact Us page](#) for non-emergency enquiries or complaints@rightfirsttimeuk.com for formal complaints. Do not send passwords, recovery codes or unnecessary confidential case records in an initial message.

This policy should be read with the Data Protection & GDPR, Governance & Transparency, Financial Controls & Expenses, Safeguarding, Complaints, Records Retention, AI and Community Standards policies, as applicable. Serious risk or danger may require immediate contact with the relevant provider, bank or authorities.

Official guidance

[NCSC – Small Organisations Guide](#)

[NCSC – Backing up your data](#)

[UK Government – Cyber Governance Code](#)

[ICO – Security guidance](#)