

Social Media Policy

Post accurately. Protect people. Stay independent.

Right First Time UK Ltd | Company number 17493370 | Updated 13 October 2026

Incorporation accepted 3 October 2026. Review at least annually and after material legal, platform or operational changes. The registered Articles of Association are unchanged.

AT A GLANCE

Official and personal accounts are different. Check evidence before posting; allow legitimate criticism; protect children and confidential information; apply extra checks to adverts and election-period material.

1. Purpose, scope and standards

This policy governs the official social-media activity of Right First Time UK Ltd (RFTUK) and the conduct of people representing it online. It covers Facebook, Instagram, X, TikTok, YouTube, LinkedIn, Threads, Bluesky, WhatsApp Channels and other platforms used by RFTUK.

It applies to the Founder, Directors, Campaign Leaders, Campaigners, Volunteers, employees, contractors and authorised contributors. Its aims are accurate information, constructive debate, safeguarding, privacy, lawful activity, cyber security and non-party political independence.

2. Official accounts and personal expression

Official accounts are created, owned or authorised by RFTUK and must use accurate organisational branding. Personal accounts remain personal: lawful political views, criticism or party membership do not automatically represent the organisation.

People in visible RFTUK roles must distinguish their personal opinions from official positions where confusion is likely. Public Membership, volunteering or leading one campaign does not, by itself, grant authority to speak for the entire organisation.

3. Posting authority, access and recovery

Only authorised contributors may publish on official accounts. Access must be proportionate to the role, with administrator privileges limited, reviewed and removed promptly on departure or loss of authority.

Use organisational ownership and recovery settings where the platform permits. Apply MFA, passkeys or the strongest practical protection; secure recovery codes and API tokens. No former contributor or external contractor should be the sole holder of account recovery access.

Never disclose passwords, tokens, IP/security information, private admin dashboards or recovery details in posts or ordinary group chats.

4. Accuracy, evidence and responsible publication

Check material factual claims against credible evidence; link primary and official sources where practical and clearly separate fact, allegation, analysis and opinion. A viral post, screenshot or short clip is not verification.

Breaking news may be labelled unconfirmed, but uncertainty must not be hidden. Accuracy, proportionality, privacy, safeguarding and public interest take priority over speed or engagement statistics.

5. Serious allegations, defamation and right of reply

Before publishing serious adverse claims about identifiable people or organisations, assess evidential strength, fairness, privacy, public-interest justification, defamation and contempt risks. A label such as “alleged” does not by itself prevent harm or legal liability.

Where appropriate, offer a reasonable opportunity to respond and represent any response fairly. A refusal or failure to comment is not proof of an allegation. Court processes require careful distinction between allegation, charge, finding, conviction, acquittal and appeal.

6. Corrections, retractions and deletion

Correct verified material errors promptly, and use a visible correction or clarification for significant mistakes. Keep a proportionate record where the original and the correction may matter.

Posts may be removed if unlawful, unsafe, misleading, privacy-invasive, materially wrong or posted in error. Removal must not be used to conceal legitimate criticism or erase accountability.

7. Privacy, direct messages and confidential records

Do not publish personal addresses, health or family details, private correspondence, case files, confidential Board information or identifying material without a valid basis and appropriate authority. Content already online is not automatically lawful to republish.

Direct messages received through an official account are organisational communications. Transfer important complaints, safeguarding disclosures, threats and evidence into the appropriate secure organisational process. Social-media messages are not a suitable channel for sending highly sensitive evidence or data-protection complaints.

8. Children, people at risk and family-court material

Before using a child's image, school, location, story or family-court information, assess consent or other lawful basis, safeguarding, privacy, reporting restrictions and possible harm. Consent from one adult does not automatically permit identifying a child or another person.

Never pressure someone facing disability, homelessness, bereavement, abuse or other vulnerability to make their story public. Family-court documents, judgments or case details must not be published simply because a party provided them; check the applicable rules, restrictions and any court order first.

9. Safeguarding, threats and urgent escalation

Escalate suspected abuse, grooming, exploitation, imminent danger or serious self-harm concerns through the Safeguarding Policy and appropriate external services. In an immediate emergency call 999. Do not turn a safeguarding disclosure into campaign publicity.

Credible threats, harassment, doxxing, stalking or impersonation may require moderation, evidence preservation, platform reports, police contact or other urgent steps. Do not confront or investigate alleged offenders personally where doing so creates risk.

10. Moderation, criticism and blocking

Official moderation should address threats, hateful or unlawful abuse, harassment, spam, exposure of private information, malicious automation and other Community Standards breaches. Options include replying, hiding/removing, restricting, muting, blocking, reporting or escalating.

Genuine criticism, negative reviews and difficult questions must not be removed merely because they are uncomfortable. Blocking must be proportionate; a workable alternative complaints route should remain available where reasonably possible. Avoid prolonged personal arguments.

11. Images, screenshots, video and intellectual property

Check permissions, rights, copyright, accuracy and context before posting media. Attribution alone is not a licence. Do not crop, edit or caption images or video so as to create a materially false impression.

Screenshots may expose private messages, usernames, security information or misleadingly omit context. Redact unnecessary identifying details and confirm authenticity, safeguarding and any court restrictions before publication.

12. AI, automation and authentic engagement

AI-generated or altered material must receive appropriate human review. Synthetic content must not falsely depict a real person saying or doing something; realistic altered content should be disclosed where legally required or where omission would materially mislead.

Approved scheduling and RSS tools may publish suitable routine content subject to review controls, but serious allegations, sensitive political material and crisis communications must not be published unsupervised. Safeguard third-party app permissions and tokens. Do not purchase fake followers, fake reviews or deceptive bot engagement.

13. Advertising, sponsorship and commercial transparency

Paid campaigns require suitable authority, accurate claims and clear identification as advertising where required by the ASA/CAP rules. Keep proportionate records of spend, audience, purpose and approving person.

Sponsorship, affiliate links, paid partnerships and advertorial material must not be disguised as independent commentary. Sponsors cannot purchase RFTUK conclusions or influence evidence findings.

14. Fundraising, memberships and PCS publicity

Fundraising messages must state the recipient and purpose accurately, including relevant platform fees or restrictions. RFTUK must not claim registered-charity status or Gift Aid entitlement without a lawful basis; do not exploit vulnerable people through misleading urgency.

Public Membership advertising must explain relevant prices, recurring payments, cancellation terms and what membership does and does not provide. Public Membership is separate from statutory company membership and PCS.

PCS social-media content must not disclose private parent, child, agreement, message, payment or safeguarding information, pressure anyone to join, or publish one parent's unverified claims about another. PCS is operated by RFTUK Ltd; parent-to-parent contributions are arranged directly and are not held or transferred by RFTUK under the stated current model.

15. Political independence and issue campaigning

RFTUK may examine public policies and the conduct of public bodies using evidence, but official accounts must not be operated as political-party or candidate campaign accounts. People with differing lawful personal political views may support RFTUK.

Political and electoral content requires extra review for accuracy, spending, audience, digital imprints and the applicable rules for non-party campaigning. Neutral civic-participation information should not be presented as party endorsement.

16. Election rules, digital imprints and platform restrictions

Before publishing or paying to promote election, referendum or recall-related material, assess whether it is regulated activity and whether an imprint, spending record, registration or other control is required. The requirements depend on the material, publisher, medium and current electoral guidance; do not assume that every organic post is exempt or every issue post automatically requires an imprint.

Follow the current rules of each platform and any AI or advertising provider used. Material may be lawful under UK law but prohibited by a particular provider. Check the Electoral Commission guidance at the time of publication.

17. Crisis communications and account compromise

Coordinate major incidents with RFTUK's Media & Press, Information Security and Safeguarding procedures. Share verified facts and practical safety information, explain uncertainty and correct changes promptly.

For a compromised social account, secure access, change credentials, revoke unauthorised sessions, preserve evidence, notify the platform, review linked services, assess personal-data breach obligations and warn affected users if appropriate.

Fraudulent impersonation may be reported; parody and lawful criticism are not automatically impersonation.

18. High-risk publication approvals

Routine authorised content may be published under delegated arrangements. Obtain additional review for serious allegations, children or vulnerable people, private legal or court material, major fundraising claims, crisis statements, paid or election-period political material, high-value sponsorship and confidential disclosures.

Approval must consider the company's actual delegated powers and registered Articles of Association. This policy does not grant authority to override those Articles or Directors' statutory duties.

19. Accessibility, engagement and fair treatment

Use plain language, meaningful alt text, captions and accessible graphics where practicable. Moderation must not penalise users for disability-related communication needs, honest disagreement, criticism or a request for reasonable adjustments.

People representing RFTUK should keep appropriate professional boundaries and should not claim credentials or authority they do not have.

20. Records, analytics, training and review

Keep proportionate records of major statements, material corrections, paid advertisements, significant moderation decisions, threats and complaints under the Records Retention & Destruction Policy. Do not archive every routine comment without a purpose.

Platform analytics must be used consistently with the Privacy Notice and applicable data-protection law. Contributors should receive role-appropriate guidance on sourcing, privacy, security, safeguarding, moderation and elections. Review this policy at least annually and sooner after material legal, platform or operational change.

21. Legal identity, operational model and complaints

Right First Time UK Ltd is a non-profit company limited by guarantee, company number 17493370; incorporation accepted on 3 October 2026. Founder, Director and volunteer roles operate on an initially voluntary/unpaid basis, with authorised expense reimbursement and any later remunerated roles governed by the registered Articles, law and formal approvals.

Complaints, moderation concerns, harmful content reports, impersonation and inaccuracies may be raised via the Contact Us page or complaints@rightfirsttimeuk.com. Serious privacy or safeguarding concerns should be referred to the appropriate dedicated process; emergency services must not be delayed while waiting for a reply.

Appendix A — Pre-Publication Social Media Checklist

The following checks should be documented proportionately for higher-risk posts.

Check	Question
Account	Is the correct official RFTUK account publishing?
Authority	Is the publisher authorised for this content?
Purpose	What is the legitimate organisational or public-interest purpose?
Evidence	Are important factual claims sourced and verified?
Allegations	Are allegation, evidence, opinion and established findings distinguished?
Right of reply	Would fairness require an opportunity for a response?
Privacy	Is unnecessary personal information or a private message exposed?
Safeguarding	Does a child or person at risk need additional protection?
Court restrictions	Are family-court, criminal-court or other reporting restrictions relevant?
Image/video rights	Are rights, context, captions and authenticity checked?
AI	Does synthetic or altered media need disclosure or further review?
Political/election	Does the material engage electoral or non-party campaigning rules?
Imprint	Is a digital imprint required for this material and publisher?
Advertising	Must the material be identified as paid, sponsored or affiliate content?
Fundraising	Are recipient, purpose, price and money-flow claims accurate?
Accessibility	Is accessible text, alt text or captioning provided as practicable?
Security	Are credentials, dashboards, private URLs and metadata protected?
Links	Do links reach the correct current and authoritative pages?
Approval	Is secondary or Director-level authorisation required?
Record	Should a correction, advertisement or major post be archived?

Official and regulatory guidance

- [Electoral Commission — digital imprints](#)
- [Electoral Commission — organic material for non-party campaigners](#)
- [ASA/CAP — identifying marketing communications](#)
- [ICO — data-protection complaints](#)
- [GOV.UK — transparency and reporting in family courts](#)
- [Defamation Act 2013](#)

Contact and complaints

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

Registered office: 82A James Carter Road, Mildenhall, IP28 7DE. PCS is operated by RFTUK Ltd; its users' private arrangements and records must never be disclosed in social posts.