

# Website Analytics Policy

Privacy-conscious website measurement and service improvement

|                        |                                                    |
|------------------------|----------------------------------------------------|
| Policy updated         | 13 October 2026                                    |
| Previous policy        | 30 September 2026                                  |
| Company                | Right First Time UK Ltd · 17493370                 |
| Incorporation accepted | 3 October 2026                                     |
| Review                 | At least annually or sooner after material changes |

Principle: Measure what helps improve the service. Do not collect more personal information simply because a tool makes it possible.

Consent first unless a genuine PECR exception applies; protect sensitive and PCS data; make choices effective; document and test the real configuration.

## 1. Purpose and scope

Right First Time UK Ltd (RFTUK) uses or may use proportionate analytics to understand website performance, accessibility, navigation and the usefulness of public information. The aim is service improvement, not to track individuals unnecessarily or build sensitive personal profiles.

This policy covers rightfirsttimeuk.com, relevant campaign and membership pages, embedded tools, online forms and the Parent Contribution Service (PCS) at pcs.rightfirsttimeuk.com. It applies to anybody authorised to configure analytics, tags, hosting reports or measurement systems for RFTUK.

## 2. Applicable law and the difference between analytics and security

RFTUK assesses analytics under the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 (PECR), and changes made by the Data (Use and Access) Act 2025. The ICO finalised its storage-and-access-technology guidance on 29 April 2026.

PECR covers technologies that store or access information on a device, including cookies, pixels, tags and comparable mechanisms. Security or server logs may have a distinct purpose and legal justification, but intrusive audience tracking must not be labelled essential simply because it is convenient.

## 3. Legitimate purposes and data collected

Permitted purposes include understanding which public resources are used, locating broken pages, measuring accessibility and performance problems, improving navigation, assessing broad campaign reach and diagnosing device compatibility.

Depending on the tool, data may include page views, approximate visit duration, referral source, browser or device type, general location, selected links, technical errors and limited IP/device information. An IP address or identifier can be personal data even without a name.

## 4. Do not send sensitive content to ordinary analytics

Analytics must be configured to prevent, so far as reasonably possible, the collection of form text, case evidence, complaint descriptions, private messages, children's details, disability or medical information, court material, safeguarding disclosures, uploaded documents, passwords and full payment-card or bank details.

Review URL paths, query strings, page titles, event parameters, search terms and referral data; these can reveal personal information even when form bodies are excluded. Use redaction, aggregation, masking and restricted events where appropriate.

## **5. Consent where PECR requires it**

Where no applicable PECR exception covers a device-access or storage technology, RFTUK must obtain valid consent before activating it. Consent must be an informed, specific and genuine positive choice: continued browsing, scrolling or silence are not consent.

Visitors should be able to accept, reject and manage non-essential technologies without manipulative design, and withdraw a consent choice as easily as they gave it. Where consent is declined, consent-based analytics must stay disabled.

## **6. Narrow statistical-purposes exception**

Under the amended PECR framework, certain first- or third-party statistical technologies may operate without consent only when all conditions of the statistical-purposes exception are satisfied: the sole purpose is aggregated statistical understanding of use to improve that website or service; users receive clear information and a simple free mechanism to object.

The exception does not cover cross-site tracking, advertising, user profiling or retaining unnecessary individual-level information after aggregation. A third party must use the information only to help improve the relevant service. An objection must stop the relevant device storage or access. RFTUK will document its assessment before relying on this exception rather than assuming that any analytics platform qualifies.

## **7. UK GDPR lawful basis and individual rights**

Even when a PECR exception applies, personal data processing requires a separate UK GDPR lawful basis and compliance with transparency, fairness, minimisation, retention, security and individual-rights rules. Where legitimate interests is used, RFTUK should record the purpose, necessity, impact on visitors and appropriate balancing safeguards.

Where UK GDPR consent is used, it must be withdrawable. Where applicable, visitors can request access, correction, restriction or erasure, and object to processing. RFTUK will assess each request according to the applicable legal basis and circumstances.

## **8. Cookie and objection controls**

The website should provide understandable controls for accepting, rejecting, managing and later changing consent-based cookies and similar technologies. A statistical-exception service must instead offer the required clear information and simple, free objection route.

Cookie preferences must be respected across applicable pages and tools, including those installed through shared headers, plugins and third-party scripts. RFTUK should test that rejecting, withdrawing or objecting actually prevents the relevant collection.

## **9. Google Analytics 4 and external analytics providers**

RFTUK may use Google Analytics 4 (GA4) or another measurement provider. In the ordinary consent-based configuration, GA4 analytics tags and associated non-essential storage/access must not activate until a visitor opts in. RFTUK must not treat GA4 as automatically eligible for the statistical-purposes exception.

Before enabling a tool, check the provider's purposes, data-sharing controls, consent settings, advertising features, processing agreements, international transfers, retention periods and any independent use of collected information. Advertising signals, remarketing and cross-site tracking must not be enabled merely because offered by default.

## **10. Analytics register and records**

RFTUK should maintain an internal register for significant analytics technologies, recording provider, purpose, information collected, tags/cookies, retention, PECR consent or exception, UK GDPR lawful basis, third parties, international transfers, advertising/profile settings, user controls and the last review date.

Changes to a provider, plugin, script, cookie banner or analytics purpose should trigger an updated register entry and, when appropriate, updated Cookie Policy and Privacy Notice wording.

## **11. Hosting logs, security and operational metrics**

Plesk/hosting reports, server access logs, firewall records and fraud-prevention systems should be distinguished from marketing or audience analytics. Access to raw logs must be restricted to authorised technical or security purposes and governed by the Records Retention & Destruction and Information Security policies.

Data must not be repurposed for individual marketing or sensitive inference simply because it was first collected for security.

## **12. Membership, donations and payment journeys**

RFTUK may measure aggregate visits and technical failures on membership, subscriber, fundraising and checkout pages but must not send personal account identifiers, membership histories, donation records, passwords, bank details or full payment-card information to ordinary web analytics.

Financial transaction records and analytics reports serve different purposes. Advertising pixels on sensitive or payment steps require particular scrutiny and must not be installed without approval and a documented legal basis.

## **13. Campaign pages, children and sensitive interests**

Engagement with campaigns or pages about benefits, disability, safeguarding, homelessness, domestic abuse, family courts, health or other sensitive subjects is not proof of a visitor's personal characteristics or political views. RFTUK must not create behavioural or political profiles from these visits.

Services likely to be used by children require stronger minimisation and avoidance of unnecessary identifiers or behavioural advertising. Aggregate campaign statistics may be useful; sensitive individual browsing profiles are not.

## **14. Parent Contribution Service (PCS)**

PCS is a service of Right First Time UK Ltd, not a separate legal entity. Its parent-to-parent contribution records and messages are private, and PCS does not itself receive, hold or transfer those child-contribution payments.

Analytics on pcs.rightfirsttimeuk.com must not capture the contents of parent messages, child details, agreements, payment records, evidence uploads, bank details or safeguarding disclosures. Sensitive PCS workflows must not be sent to advertising, remarketing, ordinary profiling or session-recording systems. A technical audit should check these protections before analytics is enabled.

## **15. Embeds, social platforms and international transfers**

Videos, embedded social posts, maps, petitions and other third-party features can set their own cookies or track visits. Non-essential tracking should be delayed, privacy-enhanced or controlled through appropriate consent where possible.

Where a provider processes personal information outside the UK, RFTUK will assess any relevant restricted-transfer requirements, processing arrangements and safeguards. A visitor leaving RFTUK for an external website will be subject to that site's separate policies.

## **16. Retention, security and access**

Identifiable analytics must not be retained indefinitely. RFTUK should set justified retention periods, shorten or aggregate individual-level records, and keep genuinely anonymised trends for longer only where useful. The provider's default retention must be reviewed.

Analytics dashboards, exports and API keys require role-based access, strong authentication, secure storage and prompt removal of access when a role ends. Exports with personal data must not be casually emailed or left on personal devices.

## **17. Advertising, profiling and unlawful installation**

Ordinary site-improvement analytics are different from paid advertising, affiliate tracking, remarketing, cross-site behavioural tracking and profiling. Any proposed advertising use needs a separate assessment, appropriate user choice and compliance with applicable law.

Volunteers, Campaign Leaders, developers and suppliers must not install unapproved analytics tags, session-replay tools, advertising pixels or similar trackers. Discovery of unauthorised tracking is treated as a potential privacy or security incident.

## **18. Privacy impact assessment and provider oversight**

Before introducing or materially changing intrusive analytics, RFTUK should assess privacy impact, necessity, foreseeable harm, supplier use, contracts, access permissions and safer alternatives. Carry out a formal Data Protection Impact Assessment where UK GDPR requires one.

Where necessary, confirm processor/controller responsibilities, suitable contractual terms, sub-processors, data sharing and international transfer safeguards before activating the tool.

## **19. Testing, incidents and corrective action**

Periodically test live browser behaviour—not only the written cookie list—to identify what tags load before choice, what happens after rejection, which data enters analytics, whether sensitive URLs or search terms leak, and whether objection or withdrawal works.

If analytics collects unintended personal information, disable or restrict the tag, preserve necessary incident evidence, seek deletion where appropriate, review provider settings and assess whether notification under data-protection law is needed.

## **20. Transparency, accessibility and reporting**

Analytics should support accessibility work, not replace direct user testing. RFTUK may publish aggregated statistics about visits, service improvements or campaign reach where the results do not reveal identifiable visitors or sensitive browsing histories.

The Cookie and Storage Technologies Policy, Privacy Notice, Accessibility Statement and Records Retention & Destruction Policy should remain consistent with the technologies actually deployed.

## **21. Enquiries, objections and complaints**

Questions about cookies, analytics and privacy choices can be raised through the RFTUK Contact Us page. Data-protection complaints should be directed to [complaints@rightfirsttimeuk.com](mailto:complaints@rightfirsttimeuk.com). Individuals may also raise eligible concerns with the Information Commissioner's Office.

The public policy describes standards and responsibilities; it does not, by itself, install a consent manager or verify that all live website scripts are compliant.

## 22. Governance, Articles and review

RFTUK Directors are responsible for governance oversight; authorised technical or operational personnel must implement and test controls appropriate to their duties. This policy operates subject to Right First Time UK Ltd's registered Articles of Association and does not amend them.

The policy will be reviewed at least annually and earlier if legislation, ICO guidance, providers, cookies, consent design, websites or RFTUK activities change materially.

## Appendix A — Practical analytics compliance checklist

Apply this checklist before deploying or materially changing analytics.

1. List every tracker, script and analytics provider, including on PCS and member pages.
2. Record each purpose, PECR consent/exception and UK GDPR lawful basis.
3. Confirm GA4 or other consent-based analytics stays off until opt-in.
4. If claiming the statistical exception, document all conditions and a free opt-out.
5. Check Accept, Reject and Manage controls on desktop and mobile.
6. Test that changing/withdrawing a choice actually disables collection.
7. Strip personal identifiers and sensitive URL parameters before tracking.
8. Exclude complaint, safeguarding, child, bank and private PCS content.
9. Review advertising, cross-site tracking, remarketing and Google data-sharing settings.
10. Confirm retention, processor terms, transfers, security and access controls.
11. Test third-party embeds, analytics events and scripts on live pages.
12. Update the analytics register, Cookie Policy and Privacy Notice after changes.

## Official and regulatory guidance

[ICO: Storage and access technologies guidance \(updated 29 April 2026\)](#)

[ICO: Exceptions, including statistical purposes](#)

[ICO: UK GDPR lawful bases and legitimate interests](#)

[ICO: Raise a data protection concern](#)

## Contact and company information

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

[Contact Us](#)

[Data-protection complaints — \[complaints@rightfirsttimeuk.com\]\(mailto:complaints@rightfirsttimeuk.com\)](#)

PCS is a service operated by RFTUK Ltd. Private child-contribution payments are made directly between parents.