# Legitimate Interests Assessment

The Reasonable Adjustment

| | |
|---|---|
| **Controller** | Kieron JH, The Reasonable Adjustment |
| **Assessment Date** | 17 February 2026 |
| **Previous Assessment** | 5 August 2025 |
| **Reason for Review** | Privacy policy updated January 2026: Formspree, Google Search Console Insights, and Bing Webmaster Tools added; retention periods aligned; third-party disclosures updated |
| **Scope** | Passive fingerprinting, analytics, contact form handling, AI-assisted correspondence, search visibility reporting, and security logging |

## 1. Purpose Test

### 1a. Why is the data processed?

This site supports advocacy, accountability, and whistleblowing, and may be a target for institutional monitoring, coordinated scraping, or attempts to deanonymise contributors. Processing serves three distinct purposes:

- Security and abuse prevention: passive fingerprinting and Cloudflare edge logging are used to detect hostile traffic patterns, flag coordinated probing, identify high-risk ASNs, and protect the integrity of the site and its contributors.
- Analytics: cookieless, aggregated usage statistics (via Plausible) are collected to understand how the site is used and to improve content and services.
- Contact and correspondence: names, email addresses, and message content are collected via direct email and via Formspree contact forms in order to respond to enquiries and provide advocacy support.
- AI-assisted correspondence: message content may be processed using OpenAI ChatGPT to assist with drafting replies clearly and efficiently.
- Search visibility reporting: aggregated search performance data is collected via Google Search Console, Search Console Insights, and Bing Webmaster Tools to understand content discoverability. This is site-level reporting, not visitor-level profiling.

### 1b. What benefit is expected?

- Detecting botnets, scrapers, and hostile access attempts without requiring cookies or logins.
- Maintaining site security and resilience against institutional overreach or suppression.
- Evidence of harassment or surveillance patterns where relevant to legal claims or accountability.
- Understanding how visitors use the site to improve content.
- Efficient and accessible correspondence management, particularly given the operator's autistic identity and need for productivity support.

- Understanding how content is indexed and surfaced in search to improve discoverability.

### 1c. Is this a legitimate interest?

Yes. Site security, abuse detection, and the protection of whistleblowers and contributors are recognised legitimate interests under UK GDPR Article 6(1)(f) and Recital 47. Responding to enquiries and improving services are well-established legitimate interests. AI-assisted correspondence is a legitimate operational interest where human oversight is maintained. Search visibility reporting is a standard, low-risk site management function.

## 2. Necessity Test

### 2a. Is the processing necessary for the stated purpose?

Yes for each purpose:

- Fingerprinting: passive, non-cookie fingerprinting is one of the least intrusive methods of identifying abusive or suspicious behaviour while avoiding the consent requirements of cookie-based solutions.
- Analytics: cookieless, aggregated analytics via Plausible is the minimum necessary to understand usage patterns. No individual profiles are created.
- Contact handling: names, email addresses, and message content are the minimum required to respond to enquiries. Technical metadata from Formspree (IP address, user agent) is collected as part of the submission process and retained in line with the provider's standard operation.
- AI assistance: message content is the minimum necessary to draft a coherent reply. Identifiers are minimised or redacted where possible.
- Search reporting: Google Search Console, Search Console Insights, and Bing Webmaster Tools provide only aggregated, site-level data. Individual visitor data is not accessed.

### 2b. Can the same result be achieved less intrusively?

Alternative methods were considered:

- IP-only logging is less effective due to VPNs, Tor, and shared addresses.
- Cookie-based tracking is more intrusive and requires consent under PECR.
- CAPTCHA systems are more discriminatory and intrusive, particularly for disabled users.
- Disabling AI assistance would reduce the operator's ability to communicate effectively and maintain productivity. Human review of all AI outputs is retained as a safeguard.

The current approach represents the minimum necessary processing for each stated purpose.

## 3. Balancing Test

### 3a. What data is collected?

- Security and fingerprinting: device type, OS version, browser version, screen dimensions, timezone, platform, IP address (used for geolocation to country level), ASN, Cloudflare PoP and protocol details, requested URL. No special category data.

- Analytics: page views, referrer, and approximate time on site, aggregated and cookieless. No individual profiles.
- Contact forms and email: name, email address, message content. Technical metadata from Formspree submissions. May contain sensitive advocacy content but not intentionally special category data.
- AI-assisted correspondence: content of messages as above, with identifiers minimised where possible.
- Search reporting: aggregated click and impression data, broad query trends. No individual visitor data.

### 3b. Could processing cause harm or distress?

The following risks were considered:

- Fingerprinting may have a chilling effect on visitors who would prefer complete anonymity, particularly whistleblowers or activists. This is a genuine tension. It is mitigated by: the cookieless, non-advertising nature of the fingerprinting; clear disclosure in the privacy policy; no individual profiling or marketing use; data minimisation and rotation; and the fact that the security purpose directly protects the same visitor group that might be concerned.
- AI processing of correspondence introduces a risk of identifiable information being processed by a third party (OpenAI) outside the UK. This is mitigated by: minimising identifiers before submission; avoiding special category data in AI tools; using temporary chat modes for sensitive topics; ensuring human review of all outputs; and relying on the UK-US Data Bridge or Standard Contractual Clauses for the transfer.
- Contact form metadata (IP address and user agent via Formspree) may be retained longer than the visitor expects. This is mitigated by disclosure in the privacy policy and a 12-month retention cap.
- Aggregated analytics and search reporting pose negligible individual risk.

### 3c. Would users reasonably expect this processing?

Given the site's explicit focus on advocacy, accountability, and whistleblowing, visitors may reasonably expect a higher degree of security scrutiny than on a typical personal website. The Privacy Policy provides clear, layered disclosure of all processing activities, including fingerprinting, AI use, and third-party processors. A changelog is maintained so returning visitors can identify what has changed.

### 3d. Opt-out and Article 21 rights

There is no practical opt-out from passive security fingerprinting, as it is necessary to deliver the service and protect it from abuse. This is analogous to server logging on any website. Visitors who require complete anonymity may use Tor or high-privacy browser configurations, which reduce fingerprinting effectiveness.
For processing based on legitimate interests, individuals retain the right to object under UK GDPR Article 21. Objections should be directed to advocacy@thereasonableadjustment.co.uk. The operator will consider each objection individually and cease processing unless compelling legitimate grounds override the individual's interests.

## 4. Safeguards and Retention

| Safeguard | Detail |
|---|---|
| **No advertising use** | No advertising profiles, pixels, or marketing cookies. Fingerprinting is strictly for security. |
| **Data minimisation** | Signals minimised; identifiers redacted before AI submission where possible; search reporting is aggregated only. |
| **Retention — fingerprinting** | Typically 6 months. Extended only where there is a specific, documented concern (e.g. hostile activity, legal claims). |
| **Retention — correspondence** | Up to 12 months; deleted sooner on request. |
| **Retention — AI tools** | Conversations kept only while relevant to the active matter, in any event no longer than 12 months. Temporary chat used for sensitive topics. |
| **Retention — Formspree** | Up to 12 months; deleted when no longer needed. |
| **Retention — search reporting** | Aggregated data retained in line with Google and Microsoft provider terms. Not individually identifiable. |
| **Human oversight (AI)** | All AI outputs reviewed and edited before use. No automated decisions with legal or similarly significant effects. |
| **Security measures** | HTTPS, 2FA on all provider accounts, device encryption, role-limited access. |
| **Third-party processors** | Cloudflare, Plausible, Formspree, OpenAI, Discord. International transfers rely on UK-US Data Bridge or Standard Contractual Clauses. |
| **Periodic review** | This assessment is reviewed whenever the Privacy Policy is materially updated. |

## 5. Conclusion

Processing across all activities described in this assessment is:

- Carried out for a legitimate interest (site security, abuse prevention, correspondence, analytics, AI-assisted productivity, and search visibility reporting).
- Necessary for that purpose, with less intrusive alternatives considered and rejected where appropriate.
- Proportionate, with risks to individuals acknowledged and mitigated through technical and organisational safeguards.

The controller therefore relies on Article 6(1)(f) of UK GDPR as the lawful basis for processing described in this assessment. Advocacy processing involving special category data relies on explicit consent under Article 9(2)(a) and is addressed separately in the Privacy Policy.