Whistleblower Privacy & Protection Policy

1. Introduction

Restore Britain (“we,” “us,” or “our”) is committed to protecting the confidentiality, privacy, and safety of individuals who choose to disclose information in the public interest (“whistleblowers”).

Restore Britain cannot provide legal advice to whistleblowers. If you are uncertain about your legal position, you should seek independent legal counsel before making a disclosure.

2. Non-Retaliation

Restore Britain will never retaliate against or disadvantage a source for making a disclosure. While we cannot control the actions of employers, government bodies, or third parties, we will take all reasonable steps to protect the confidentiality and safety of those who come forward.

This Policy explains how we collect, use, and protect the information you provide when reporting concerns. We operate in line with the UK General Data Protection Regulation (GDPR), the Data Protection Act 2018, and recognised best practices for whistleblowing protection.

Because disclosures may involve sensitive or high-risk information, we prioritise anonymity, security, and your right to choose how much personal information you share.

3. Who We Are

Restore Britain is an independent body that receives and reviews whistleblower disclosures. For the purposes of GDPR, we are the data controller of any personal data you choose to provide.

Contact: ContactRestoreBritain@protonmail.com

4. What Data We Collect

Depending on what you choose to provide, we may collect:

- **Contact Information** – name, email, or phone number (if you give it).
- **Disclosure Content** – the details of your whistleblowing report and any supporting evidence.
- **Sensitive Data** – if contained in your disclosure (e.g. health, political opinions).

- **Technical Data** – minimal device or metadata when using online tools (we minimise retention of this).

We accept anonymous disclosures. You do not need to provide identifying details.

5. How We Collect Your Data

- **Directly from You:** via submission form, encrypted email, Signal, or other secure channels.

- **Automatically:** limited technical data through website cookies or server logs (see Section 14).

- **Third Parties:** only if you authorise someone else to submit on your behalf.

For your protection, we encourage the use of encrypted channels. We cannot guarantee the security of unencrypted email in transit.

6. Editorial Safeguards & Defamation Defence

- Restore Britain ensures all reporting is evidence-based.

- Individuals or organisations facing serious allegations will be given a fair opportunity to respond unless doing so would create imminent risk of harm.

- Responses will be considered in good faith and included where relevant.

- We recognise the Section 4 Defamation Act 2013 public interest defence, requiring reasonable belief that publication is in the public interest, supported by adequate inquiries and checks.

7. Legal Basis for Processing

- **Explicit Consent:** where you choose to provide personal data.

- **Legitimate Interests:** to assess, verify, and act on disclosures while protecting your confidentiality.

- **Legal Obligation:** where disclosure is required by law (e.g. safeguarding, national security).

We do not process data for marketing, profiling, or unrelated purposes.

8. How We Use Your Data

- To assess disclosures and take appropriate action.
- To maintain contact with you (if details are provided).
- To prepare anonymised reports excluding personal identifiers.
- To meet legal or regulatory obligations.

9. Sharing Your Data

We will not share your personal data without your consent except where:

- Required by law or court order.
- Safeguarding or immediate risk issues make disclosure necessary.
- Anonymised, aggregated data is used in reporting.

Where safeguarding or imminent risk is identified, disclosure will be limited strictly to what is necessary.

10. Data Security & Access Controls

- Encrypted storage and secure servers.
- Access limited to authorised personnel under strict confidentiality.
- Regular security reviews and risk assessments.

11. Data Retention & Deletion

- Personal disclosures are retained only as long as needed (maximum 18 months unless extended with your consent).
- Fully anonymised reports may be stored indefinitely.
- If you submit anonymously, deletion or amendment may not be possible.
- Material retained beyond 12 months despite being unused will be documented, including justification (e.g. legal defence purposes).
- Material suspected of falling under the Official Secrets Act 1989 will be quarantined and securely deleted unless retention is ordered by a court.

12. Complaints and Objections (GDPR Article 21)

- Restore Britain recognises the right to object to processing under Article 21.
- Complaints are formally logged and reviewed by the Head of Investigations and Legal Counsel.
- A written record is maintained of the complaint, evidence considered, and reasoning.
- Logs are retained for accountability and may be inspected by the ICO.

13. Your Rights under GDPR

You have rights to:

- Access your data
- Rectify inaccuracies
- Erase data (“right to be forgotten”)
- Restrict or object to processing
- Withdraw consent
- Complain to the ICO

14. Cookies & Website Use

Our website may use cookies strictly necessary for security and functionality.
Analytics cookies are optional and require explicit consent.

15. International Transfers

We do not routinely transfer data outside the UK or EEA.
Some service providers (e.g., Typeform) may process data abroad; in those cases, approved safeguards such as adequacy decisions or standard contractual clauses are applied.

16. Changes to this Policy

We may update this policy to reflect changes in law or best practice.
The latest version will always be available on our website.

17. No Legal Advice

Restore Britain does not provide legal advice to whistleblowers.
Individuals should seek independent legal counsel before making a disclosure if unsure of their rights or risks.

18. Official Secrets Act (OSA) Warning

- The OSA 1989 makes it a criminal offence to disclose certain categories of information.
- The OSA has **no public interest defence**.
- Restore Britain cannot protect whistleblowers from legal liability under the Act.
- Suspected OSA material will be quarantined and securely deleted unless a court orders otherwise.

Whistleblowers must ensure they are not disclosing OSA-prohibited information.

19. Complaints and Objections (duplicate section integrated)

This section is already covered in Section 12.

20. Breach Notification

- Restore Britain has procedures to identify and assess potential data breaches.
- Where risk exists to individuals' rights or freedoms, the ICO will be notified within 72 hours.
- Affected individuals will be informed where high risk is identified.
- All breaches and decisions (including where the journalism exemption applies) are documented offline.

21. Tier 3 Physical Submissions (PO Box System)

Tier 3 is an enhanced security route for whistleblowers who cannot risk digital transmission and choose to send information via physical mail. These disclosures are treated as highly sensitive, and Restore Britain applies strengthened confidentiality, handling, and security procedures to protect both the whistleblower and the integrity of the material.

21.1 What You May Send

- Printed documents
- Handwritten notes

- Photographs or physical evidence
- Storage media (USB drives, SD cards, CDs)

We do not attempt to identify anonymous senders.

21.2 PO Box Retrieval & Handling

- Mail collected at irregular intervals
- Retrieval, transport, and opening only by authorised personnel
- Transported in sealed evidence pouches
- No digital record of sender details (e.g. postmarks, handwriting)

21.3 Opening & Examination

- Gloves worn at all times
- Packaging separated and stored independently
- Submissions categorised as documents, handwritten notes, storage media, or high-risk
- Storage media quarantined and malware-checked in isolation
- Only minimum examination prior to secure storage

21.4 Storage & Access Controls

Tier 3 submissions are stored:

1. In a locked cabinet;
2. Inside a secure, controlled-access room.

All access logged in a paper-only chain of custody.

21.5 Retention & Destruction

- Retained only as long as necessary (max 18 months unless justified otherwise)
- Destruction via cross-cut shredding or physical destruction of media

- Two authorised handlers must sign the destruction log

21.6 High-Risk or OSA Material

- Immediately quarantined
- Reviewed minimally to identify nature
- Securely destroyed unless a lawful order requires retention

Restore Britain cannot protect whistleblowers from OSA liability.

21.7 Editorial & Investigative Use

Tier 3 material:

- Verified using corroboration, OSINT, and relevant FOIs
- Circulated internally only in redacted/anonymised form
- Never referenced explicitly in FOIs
- May guide investigative direction without implying origin

21.8 Staff Conduct Requirements

All Tier 3 handlers must:

- Sign enhanced confidentiality and evidence-handling agreements
- Follow the two-person rule for retrieval, opening, review, and destruction
- Report interference or unauthorised access
- Undertake annual security and legal-risk training

22. Contact

For questions or data requests: **ContactRestoreBritain@protonmail.com**