Subject: Urgent Request for Case Re-Review – ICO Reference IC-188010-V0J0

Dear Sir/Madam,

I am formally requesting an **urgent re-review** of my data protection complaint against Herefordshire Council, under **ICO Reference IC-188010-V0J0**, due to the serious failures of both **Rachel Webster (case reviewer)** and **Alison Fletcher (investigator)** in properly applying the **UK GDPR** and **Data Protection Act 2018 (DPA 2018)** to this case.

Your decision to dismiss my complaint and failure to hold Herefordshire Council accountable have **directly enabled and encouraged further data protection and other abuses**. Most significantly, your inaction permitted the **destruction of crucial supporting evidence**, irreparably harming my ability to seek legal redress.

As the UK's data protection authority, the ICO has a statutory duty to investigate complaints of data protection breaches under Section 165 of the Data Protection Act 2018. By dismissing my complaint, the ICO has failed to meet this duty, allowing Herefordshire Council to continue their unauthorised activities with impunity.

ICO Failures & Their Consequences

1. ICO's Failure to Recognise Unlawful Data Processing – GDPR Article 6 Violation
It is an established fact that Herefordshire Council **accessed my personal website unlawfully over 150 times**—many of these instances occurring **after security restrictions were placed to block them**.

Under **Article 6(1) GDPR**, all data processing must have a **valid legal basis**. However, neither **Rachel Webster nor Alison Fletcher**, properly investigated this **fundamental requirement**.

Furthermore, it has now been conclusively established that Herefordshire Council did not have **RIPA (Regulation of Investigatory Powers Act) authorisation**, making their actions **completely unlawful**, aside from conflicting with their own policy documents. Despite this, the ICO **failed to recognise this as a GDPR violation**.

2. ICO's Misrepresentation of the Scale of the Breach – Failure to Accurately Assess Evidence

Herefordshire Council claimed to the IPT that **only five visits** were made by Herefordshire Council, stating:
"Four separate officers of the council. One of the officers has since left the council, and one is unnamed. The other two officers do not recall visiting the website or why they would have done so. Both officers have also confirmed that they did not capture any evidence from the website."

However, in reality, the **number of visits to the website alone exceeded 150**—as the ICO was made aware—and significant amounts of data were **accessed and copied,** some of which the ICO was made aware via my providing evidence of council copies.

Your failure to acknowledge the **full extent of the breach** means:

- **The Council's misconduct was significantly downplayed.**
- **The ICO's investigation was wholly inadequate**, leading to a wrongful decision.
- **The Council was effectively given impunity**, encouraging them to continue breaching data protection laws, as I have recently demonstrated occurred, caused by one of their solicitors.

This misrepresentation is a clear failure of duty by the ICO and a **violation of my rights under Article 5(1)(a) GDPR** (**lawfulness, fairness, and transparency**).

3. ICO's Decision Enabled the Destruction of Crucial Evidence – Direct Harm to My Legal Redress
By refusing to act, the ICO **allowed Herefordshire Council to destroy critical evidence** that I needed for legal proceedings.

The ICO's dismissal of my complaint allowed Herefordshire Council to:

- **Delete internal records** that could have proven the extent of their unlawful website access, without doubt, complimenting my evidence.
- **Erase logs and audit trails** that would have supported legal action under GDPR.
- **Continue their unauthorised activities**, knowing the ICO would take no action.

This is a **direct breach of Article 5(1)(f) GDPR** (**integrity and confidentiality**), which requires data controllers to safeguard data from unauthorised destruction—yet the ICO has failed to uphold this fundamental principle.

Additionally, under **Section 171 of the Data Protection Act 2018**, it is a **criminal offence to alter, erase, or conceal personal data to**

prevent disclosure. By failing to act, the ICO has **allowed Herefordshire Council to violate this legal provision with impunity**.

4. ICO's Failure to Address Security Breaches – GDPR Article 32 Violation

A major failing in your review was the refusal to acknowledge that Herefordshire Council **deliberately bypassed security controls** on my website and social media to gain unauthorised access.

- **Article 32(1) GDPR** mandates that organisations implement appropriate technical and organisational measures to ensure the **security of personal data**, including **preventing unauthorised access** and ensuring accountability for staff actions.
- Herefordshire Council **deliberately circumvented these measures**, demonstrating **intentional misconduct**—yet the ICO **failed to recognise this as a violation**.

Key GDPR Violations Under Article 32

1. Failure to Prevent Unauthorised Access & Security Failures

- Herefordshire Council employees **repeatedly accessed a third-party website (my website) without lawful authorisation**.
- This raises serious concerns about whether Herefordshire Council had adequate **security controls** in place to prevent unauthorised staff access to external data sources, given they had no authorisation to do so.
- The failure to restrict, monitor, or control such access demonstrates either **gross negligence** or a deliberate attempt to override security controls.

2. Failure to Log & Monitor Staff Activity

- **Article 32(1)(d) GDPR** requires controllers to ensure the **confidentiality, integrity, availability, and resilience** of processing systems.
- Herefordshire Council **failed to adequately log staff access** to my website and their copying of data, destroying data with the knowledge it would be and was requested. Repeatedly refusing to provide said data for legal redress represents a **serious breach of Article 32 GDPR** and a failure of internal security controls.

3. ICO's Failure to Recognise the Security Breach

- The ICO's **refusal to acknowledge this breach** effectively grants public authorities a **free pass** to override digital security controls, setting a dangerous precedent that undermines GDPR protections.
- This also creates a potential legal loophole where public bodies can bypass security protections, access data without authorisation, delete or destroy evidence and potentially avoid accountability, as Herefordshire Council has done.

5. ICO's Misdirection to the IPT – Misapplication of RIPA
The ICO **wrongly advised me** to escalate my complaint to the **Investigatory Powers Tribunal (IPT)**, falsely implying this was a **surveillance issue under RIPA**.

However, the IPT confirmed that:

- Herefordshire Council **DID NOT have RIPA authorisation**, therefore not in their remit to investigate.
- The IPT **does not investigate pure data protection breaches**, meaning this matter always fell within the ICO's jurisdiction.

By misdirecting me, the ICO:

- **Delayed my access to justice.**
- **Allowed Herefordshire Council time to destroy crucial supporting evidence.**
- **Avoided taking action on a clear data protection breach.**
- **Allowed further harassment and rights abuses to occur.**

Formal Request for Re-Review & Investigation

Given the clear failings of both Rachel Webster and Alison Fletcher, I **respectfully request** that the ICO reopens my case and conducts a **full re-investigation** addressing:

1. The **Council's lack of lawful basis** for repeated, unauthorised access to my website (**Article 6 GDPR violation**).
2. The **ICO's misrepresentation of the scale of the breach** (150+ unauthorised visits, not just 5).
3. The ICO's **failure to recognise evidence destruction** and its impact on my legal redress.
4. The Council's **deliberate bypassing of security measures**, violating **Article 32 GDPR**.
5. The **ICO's failure to prevent continued breaches**, which encouraged Herefordshire Council's misconduct.
6. The ICO's **wrongful advice to refer the matter to the IPT**, when it was clearly a data protection issue.

Lastly, I would like you to record that Herefordshire Council have extended their punitive **'unreasonable behaviour' policy**, which I do not regard as lawful. This, in part, is for the assistance the ICO gave regarding a more recent and separate case (**ref: IC-325212-Z1**[redacted]) in obtaining some of the information I had been pursuing, repeatedly asked for, and was entitled to under GDPR.

I look forward to your response and the likely **acceptance of the previous case review, due to the harm the original misguided decision and review caused.**

Sincerely

[redacted]

Mr C Bury

Key Points Summary on Separate Page Below

Key Points Summary: ICO Case Re-Review Request (IC-188010-V0J0)

- **ICO Failures**:
  - **Failure to recognise unlawful data processing**: Over 150 unauthorised visits to my personal website by Herefordshire Council without a valid legal basis (Article 6 GDPR violation).
  - **Misrepresentation of breach scale**: ICO incorrectly assessed the extent of Herefordshire Council's misconduct, downplaying 150+ visits as only 5.
  - **Allowed destruction of evidence**: ICO's inaction led to the deletion of critical data by Herefordshire Council, harming my legal redress (Article 5(1)(f) GDPR).
  - **Failure to address security breaches**: ICO failed to act on deliberate bypassing of website security measures by Herefordshire Council, violating Article 32 GDPR.
  - **Misdirection to the IPT**: ICO wrongly referred the matter to the Investigatory Powers Tribunal, despite it being outside their remit.
- **Consequences of ICO's Failures**:
  - Encouraged continued GDPR breaches by Herefordshire Council.
  - Enabled destruction of critical evidence, further obstructing my access to justice.
  - Created a dangerous precedent for public bodies bypassing digital security controls and avoiding accountability.
- **Formal Request**:
  - Reopen the case and conduct a full investigation into:
    1. The Council's lack of lawful basis for accessing my website (Article 6 GDPR).
    2. ICO's failure to recognise the scale of the breach (150+ visits).
    3. Evidence destruction permitted by the ICO.
    4. Security breaches and deliberate circumvention by Herefordshire Council (Article 32 GDPR).
    5. ICO's wrongful advice to escalate the matter to the IPT.
  - Record Herefordshire Council's punitive 'unreasonable behaviour' policy and its effects on my rights.