HEDDLU
GOGLEDD CYMRU
NORTH WALES
POLICE

Response Date:07/04/2026

2026/317 - cloud-based intelligence suites, third-party OSINT tools, and online-research platforms

In response to your recent request for information regarding;

I am requesting recorded, high-level information held by the force about its use of cloud-based intelligence suites, third-party OSINT tools, and online-research platforms. No operational methods, technical detail, or sensitive system design is sought.

1. RIPA Considerations - Repeated Lookups & Surveillance Thresholds Please provide any recorded, high-level guidance on:
*** how the force determines when repeated online lookups on the same individual may constitute directed surveillance under RIPA 2000;**
*** how authorisation requirements are considered when multiple staff or teams conduct online checks on the same subject;**
*** any guidance identifying when online research may require RIPA authorisation.**

2. Inter-System Authorisation, Data Flows & Use of IPA-Acquired Data Please provide any recorded high-level information regarding:
*** governance of data acquired under the Investigatory Powers Act 2016 (such as communications data or CDRs) when processed in internal analytical systems, and when identifiers from this material are exported to external OSINT tools;**
*** how purpose-limitation requirements under IPA 2016, DPA 2018 and UK GDPR are maintained when IPA-acquired material or derived identifiers are used in third-party platforms;**
*** safeguards or data-protection processes intended to prevent collateral intrusion, secondary use, function creep, or inappropriate movement of identifiers between systems;**
*** how lawful authority is maintained when staff use IPA-derived identifiers within OSINT systems;**
*** any guidance describing when online activity involving IPA-derived identifiers may reach the threshold of directed surveillance requiring RIPA approval.**

3. Cloud-Hosted Analytical Platforms, Cross-Case Search & Multi-Agency Access
3.1 Cloud-Hosted Analytical Platforms
Any high-level information covering:
*** governance, policy, or guidance for the use of cloud-hosted intelligence or analytical systems;**
*** how necessity and proportionality requirements under IPA 2016 are met when handling IPA-derived material;**
*** recorded safeguards preventing unauthorised access, function creep or use of data in unrelated cases.**
3.2 Cross-Case or Multi-Agency Search

Please provide high-level information on:
*** whether systems used by the force support cross-case, cross-force, or multi-agency search;**
*** how IPA-derived identifiers are prevented from becoming accessible to other cases, departments, or agencies without renewed lawful authority;**
*** any governance processes for limiting or approving cross-case or multi-agency access.**
3.3 Access Control in Shared Environments
*** how access within shared or multi-agency cloud environments is authorised, audited and restricted;**
*** how compliance with IPA 2016, DPA 2018, UK GDPR and RIPA 2000 is maintained when users can search across multiple datasets;**
*** how risks of collateral intrusion are mitigated in shared systems.**
3.4 Exporting Identifiers to External OSINT Tools
*** how the force ensures IPA-derived identifiers are only exported to external OSINT tools when lawfully justified;**
*** any recorded guidance preventing unauthorised onward sharing;**
*** oversight or approval processes governing the export of identifiers from cloud platforms to OSINT tools.**

4. Hosting & Data Location Information
Please provide any recorded high-level information on:
*** whether OSINT or online-research tools used by the force are hosted in the UK or overseas;**
*** any general supplier information relating to data handling, processing or storage;**
*** any considerations recorded regarding cross-border data-processing risks.**

5. Third-Party System Integrations
Please confirm whether the force holds any recorded information indicating that third-party OSINT or online-investigation tools integrate with internal systems. If so, please provide:
*** the system name;**
*** confirmation of integration;**
*** a high-level description of the purpose of that integration, including whether identifiers or reference data are exchanged.**

REQUEST 2:

What would you like to know?: I am requesting the following recorded information, policies and guidance held by the force in relation to its use of cloud-based intelligence suites, third-party open-source intelligence (OSINT) and online-research tools.

1. OSINT Policies & Guidance

Please provide any publicly releasable policies, guidance documents, or high-level governance frameworks relating to:
the force's use of open-source intelligence; online research conducted by officers or staff; browser-based or third-party OSINT platforms; training, competency requirements, or authorisation levels for personnel conducting OSINT or online research; monitoring or auditing of user activity when accessing OSINT or online-investigation tools.

I am not requesting operational SOPs, tactical guidance, investigative methodology, or sensitive material whose release would prejudice law enforcement.

2. Training & Monitoring of Staff Using OSINT / Online-Research Tools Please provide any recorded information, high-level guidance, or publicly releasable material held by the force regarding:
training requirements for staff using OSINT or online-research tools; whether the force records training completion, competency, or accreditation for OSINT practitioners; any high-level audit, oversight, or monitoring processes relating to staff use of online-research tools (e.g., frequency monitoring, repeated checks on the same individual, or supervisory review).

No operational audit logs or workflow descriptions are requested.

3. NPCC Internet Intelligence & Investigation (III) Guidance Please confirm: whether the force holds a version of the NPCC Internet Intelligence & Investigation (III) Strategy more recent than the publicly available version; whether the force supplements the NPCC III Strategy with any internal guidance relevant to online research or OSINT; any documents the force uses to ensure compliance with NPCC III guidance.
Only publicly releasable material is requested.

Our information is set up and searchable for our policing purposes. To obtain the information in the format you have requested would involve manually reviewing each record on our force system. The cost of providing you with the information is above the amount to which we are legally required to respond i.e. the cost of retrieving the information exceeds the 'appropriate level' as stated in the Freedom of Information (FOI) Fees and Appropriate Limit regulations 2004.

Therefore, in accordance with the FOI Act 2000 the information you have requested is exempt under Section 12 (1), and this letter acts as a Refusal Notice under section 17 (5) of the legislation.

THIS INFORMATION HAS BEEN PROVIDED IN RESPONSE TO A REQUEST UNDER THE FREEDOM OF INFORMATION ACT 2000, AND IS CORRECT AS AT 07/04/2026.