



Response Date:20/02/2025

2025/101 - Data breaches per police constabulary

In response to your recent request for information regarding;

- 1. Can I have your records about sales of personal data from 2023 (01.01.2023) to 2024 (31.12.2024), including trading partners and money earned from transactions?**

No information held.

- 2. Do you use tracking cookies on your website, and can I have a list of third parties that you share personal data with?**

Tracking cookie information on our website is provided here: [Cookies | North Wales Police](#)

It is a page created and managed by the national Single Online Home team so we have no access or control over what cookies they allow / use to provide the service.

- 3. Have you received any complaints about how you handle personal data? This includes collecting, storing, sharing or selling, as well as wider processing practices.**

Please find below data in relation to the number of Rights Requests (for rectification, retention and deletion) received under the Data Protection Act:

2023

	Rectification	Deletion	Retention
Number of requests	9	13	1

2024

	Rectification	Deletion
Number of requests	14	31

Please note: an individual may have asked for more than one action per request e.g. deletion and rectification.

Please can I view records about these complaints for 2023 and 2024?

The content of any requests is personal information and would not be disclosed.

The information you have requested constitutes personal data of which you are not the subject and disclosure of the information to a member of the public otherwise than under the Data protection Act 2018 would contravene the data protection principles.

Section 40 is a class based exemption, therefore it is not necessary to evidence harm caused by disclosure.

The data protection rights of a third party would be breached by disclosure, therefore section 40(2) is an absolute exemption and a Public Interest Test is not necessary. This is so because personal data is governed by another law (The Data Protection Act 2018) and there are two elements to this exemption.

All requests made under FOIA are applicant blind. A request must be treated as such and a public authority will always view any disclosure as into the public domain. Thus North Wales Police must be satisfied that any release of information will be potentially available to the general public. It is therefore on this basis that the following is relevant.

The first element of this exemption is engaged if the information requested constitutes personal data and is made by the data subject. The information will be covered by section 40(1) and the request will be dealt with under the Data Protection Act, rights of access.

The second element of this exemption is engaged if the personal data is about someone other than the applicant. Where someone makes an application for information other than the data subject, disclosure of that information will often constitute a breach of the Data Protection Act covered by section 40(2).

Personal data is regulated under the principles of the Data Protection Act and when information contains personal data about a third party it can only be refused if disclosure would breach any of the data protection principles.

As previously highlighted, any disclosure under the FOIA is a public disclosure and release of the identity of an individual would breach principles 1 & 2 of the Data protection Act 2018.

These principles require that: 1) the processing of personal data for any of the law enforcement purposes must be lawful and fair and 2) the law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate.

'Data subjects' are provided with certain legal enforceable rights under the Data Protection Act 2018. The fact that the information is held for lawful policing purposes, disclosing it onwards would breach the principles, and would be incompatible with the data subject's right that their data is held securely. By disclosing this information, the force could be subject to enforcement proceedings under the act if it breaches any of those principles.

Therefore, in accordance with the Freedom of Information Act 2000, this letter acts as a Refusal Notice under section 17 (1) of the legislation.

4. How many subject access requests did you receive in the period 2023-2024, broken down by year?

2023- 459

2024- 568

What types of personal data did they typically receive? For example email addresses, home addresses and telephone numbers?

We do not keep a record of the data typically received/disclosed.

They were all requests for Personal Data.

5. How many data breaches have you experienced for the past 5 years (broken down by each year)?

Data Breaches:

- a. 87 - 2020
- b. 92 - 2021
- c. 78 - 2022,
- d. 71 - 2023,
- e. 116 - 2024
- f. 4 - 2025 (Up to now)

We can also neither confirm nor deny whether we hold any further information in relation to your request as the duty in Section 1(1)(a) of the Freedom of Information Act 2000 (the Act) does not apply by virtue of the following exemptions:

Section 24(2) – National Security

Section 31(3) – Law Enforcement

Harm in Confirming or Denying that Information is held

To confirm or deny whether any further information is held in respect of successful cyber-attacks resulting in Data Breaches would provide actual knowledge that where an attempt has been made, it has or has not been successful. Confirming that such information is not held may assist potential attackers by indicating that an attack had gone undetected. Equally, confirming information is held would enable understanding of where attacks have been successful, and possible weaknesses exist. Attackers may then be able to tailor their methods to increase their chances of success.

To confirm or deny whether information is held in respect of any leaked data as a result of an attack would, in effect, confirm that there had been successful cyber-attacks made against North Wales Police, which would present harm as detailed above.

Furthermore, in order to counter criminal and terrorist behaviour it is vital that the police and other agencies have the ability to work together, where necessary covertly, in order to obtain intelligence within current legislative frameworks to ensure the arrest and prosecution of offenders who commit or plan to commit acts of terrorism, whereby their modus operandi may involve cyber-attacks on secure databases. In order to achieve this goal, it is vitally important that information sharing takes place with other police forces and security bodies within the United Kingdom in order to support counter-terrorism measures in the fight to deprive terrorist networks of their ability to commit crime. To confirm or deny specific details of any breaches of information technology and security would be extremely useful to those involved in terrorist activity as it would enable them to map vulnerable information security databases.

Public Interest Considerations

Section 24(2) National Security

Factors in favour of confirming or denying that information is held

The public are entitled to know how public funds are spent and how resources are distributed within an area of policing. To confirm information is held regarding successful cyber-attacks causing Data Breaches would enable the general public to hold the police to account ensuring all such breaches are recorded and investigated appropriately. With the call for transparency of public spending this would enable improved public debate.

Factors against confirming or denying that information is held

Security measures are put in place to protect the community we serve. As evidenced within the harm to confirm whether any cyber-attacks have been successful would highlight to terrorists and individuals intent on carrying out criminal activity vulnerabilities within the police which could be further exploited.

Taking into account the current security climate within the United Kingdom, no information (such as the citing of an exemption which confirms information pertinent to this request is held, or conversely, stating 'no information is held') which may aid a terrorist should be disclosed. To what extent this information may aid a terrorist is unknown, but it is clear that it will have an impact on a North Wales Police's ability to monitor terrorist activity.

Irrespective of what information is or isn't held, the public entrust the Police Service to make appropriate decisions with regard to their safety and protection and the only way of reducing risk is to be cautious with what is placed into the public domain.

The cumulative effect of terrorists gathering information from various sources would be even more impactful when linked to other information gathered from various sources about terrorism. The more information disclosed over time will give a more detailed account of the tactical infrastructure of not only a force area but also the country as a whole.

Any incident that results from such a disclosure would, by default, affect National Security.

Section 31 – Law Enforcement

Factors favouring confirming or denying that information is held

Confirmation that information exists relevant to this request would lead to a better informed public which may encourage individuals to provide intelligence in order to reduce such security breaches.

Factors against confirming nor denying that information is held

Confirmation or denial that information is held in this case would suggest the police take their responsibility to protect information and information systems from unauthorised access, destruction, etc., dismissively and inappropriately.

Balancing Test

The points above highlight the merits of confirming or denying the requested information exists. The Police Service is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. As part of that policing purpose, information is gathered which can be highly sensitive relating to high profile investigative activity. Weakening the mechanisms used to monitor any type of criminal activity, and specifically terrorist activity would place the security of the country at an increased level of danger.

In addition anything that places that confidence at risk, no matter how generic, would undermine any trust or confidence individuals have in the Police Service. Therefore, at this moment in time, it is our opinion that for these issues the balance test favours neither confirming nor denying that information is held.

Therefore, in accordance with the Freedom of Information Act 2000, this letter acts as a Refusal Notice under section 17 (1) 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 19/02/2025