

c/o PO BOX 481
Fareham
Hampshire
PO14 9FS

Tel: 02380 478922

Email: npcc.foi.request@npfdu.police.uk

20/02/2026

FREEDOM OF INFORMATION REQUEST REFERENCE NUMBER: 2705/2026

Thank you for your request for information regarding crimes and incidents reported to the Police's Parliamentary Liaison and Investigation Team (PLAIT), which has now been considered.

Applicant Question:

I would like to submit an FOI request. Please could you come back to me with this information:

The number of crimes and incidents reported to the Metropolitan Police's Parliamentary Liaison and Investigation Team (PLAIT) involving Members of Parliament (MPs), broken down by calendar year for:

I am writing to make two FOI requests.

1) I would like to know how many crimes were reported to the Parliamentary Liaison and Investigations Team by year from 2019- to the end of 2025.

I would like the information to be broken down by crime reported i.e stalking, harassment, abuse. I believe you released this data up until 2024 previously here so I would like the data for 2025 to be added:

<https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/disclosure-logs/operations-coordination-committee/2024/175-2024-npcc-plait-data-28062024.pdf>

2) I would also like to know how many crimes have been reported by MPs specifically by year, relating to crimes committed against themselves, as well as seeing a breakdown of the types of incidents reported i.e stalking, harassment, abuse

For background, in 2019 Neil Basu told the Joint Committee on Human Rights that in 2017 151 crimes were reported by Members of Parliament across the country, and in 2018 there was an increase of 126% to 342 crimes. I would like to know how many crimes were reported by MPs in subsequent years (2019, 2020, 2021, 2022, 2023, 2024, 2025).

Please break the numbers down by crime type (e.g. harassment, malicious communications, criminal damage, threats to kill, etc.).

I recently received a very good response from you for a similar FOI request. This one is different as it includes all the crimes for 2025, rather than a partial record running up to October.

NPCC Response:

The NPCC does hold information captured by your request.

1. National data reported to the Metropolitan Police's Parliamentary Liaison Team (PLAIT), broken down by crime type, has been attached to the response letter.

The total numbers reflect the volume of reported crimes however please note that some of the crime type breakdowns have been withheld citing Section 40(2) Personal Information.

In addition please note that although held as PLAIT data at the time of the request, the entry 'Rape of a female' is not PLAIT data and has since been removed.

The NPCC can neither confirm nor deny whether any other information is held by virtue of Section 30(3) Investigations, Section 31(3) Law Enforcement & Section 40(5) Personal Information.

- Section 30 is a class based qualified exemption and the public interest considerations must be articulated.
- Section 31 is a prejudiced based qualified exemption and the prejudice (harm) of confirming or denying whether information is held must be articulated as well as the public interest considerations.
- Section 40 is an absolute exemption and there is no requirement to evidence the harm of consider the public interest.

For further information on the legislation, please see Annex A.

2. The NPCC does not hold a total for how many crimes have been reported specifically: 'by MPs, relating to crimes against themselves' as this level of breakdown is not held within the collated PLAIT data returned from forces.

In wishing to explain further, crime/incident data is shared with PLAIT if it is related to an MP or their families and their staff/office members and it is not mandatory as part of the return to provide this specific level of detail, although some forces might provide it via a free text box.

Whilst you may wish to submit a follow up request for what is held within these free text boxes, please note that due to the way information is stored, manual searches would be required and owing to the volume of information held, this is likely to engage Section 12 Cost.

Yours sincerely

Freedom of Information Officer & Decision Maker

www.npcc.police.uk

COMPLAINT RIGHTS

Internal Review

Any request for an internal review will be acknowledged and responded to, based on the specific wording of your initial request only.

We ask that any rationale to request an internal review, does not include any requests for new information and ask that these be submitted by separate email. We will acknowledge as a new request and may aggregate to your initial request in compliance with the legislation.

If you are dissatisfied with the response you have been provided with in compliance with the Freedom of Information legislation, you can lodge a complaint with NPCC to have the decision reviewed within 40 working days of the date of this response.

The handling of your request will be looked at by someone independent of the original decision and a fresh response provided.

It would be helpful, if requesting a review, for you to articulate in detail the reasons you are not satisfied with this reply.

If you would like to request a review, please write or send an email to NPCC Freedom of Information, c/o PO Box 481, Fareham, Hampshire, PO14 9FS.

Annex A

Section 17 of the Freedom of Information Act 2000 requires the NPCC, when refusing to provide information by way of exemption in question and (c) states why the exemption applies. In accordance with the Freedom of Information Act 2000 this letter acts as a refusal notice to those aspects of your request.

Legislation - Section 40 Personal Information

(1) Any information to which a request for information relates is exempt information if it constitutes personal data of which the applicant is the data subject.

(2) Any information to which a request for information relates is also exempt information if
(a) it constitutes personal data which does not fall within subsection (1), and
(b) the first, second or third condition below is satisfied.

(3A) The first condition is that the disclosure of the information to a member of the public otherwise than under this Act—

(a) would contravene any of the data protection principles, or

(b) would do so if the exemptions in section 24(1) of the Data Protection Act 2018 (manual unstructured data held by public authorities) were disregarded.

(3B) The second condition is that the disclosure of the information to a member of the public otherwise than under this Act would contravene Article 21 of the GDPR (general processing: right to object to processing).

Any information to which a request for information relates is also exempt information if it constitutes personal data which do not fall within subsection (1), and either the first or the second condition is satisfied.

S40(2) applies to third party personal data. Any release would breach the data protection principles contained within the Data Protection Act 2018. S40(2) has been engaged by virtue of S40(3)(a)(i). Any disclosure of withheld information would breach the first data protection principle of fair and lawful processing.

This is an absolute exemption and there is no requirement to apply the public interest test.

To neither confirm nor deny with any other information is held:

The College of Policing has an Authorised Professional Practice on Intelligence Management which is a national standard adhered to by all police forces across England and Wales. These are four products which are the deliverables of intelligence led policing. Each product has a defined purpose and provides recommendations for making decisions and options for action. These four products are strategic assessment; tactical assessment; subject profile and problem profile.

This APP can be viewed [here](#).

It is a business process with an intention to provide focus to operational policing and to achieve a disproportionately greater impact from the resources applied to any problem. It is dependent on a clear framework of analysis of information and intelligence allowing a problem solving approach to law enforcement and crime prevention techniques.

In addition, the College of Policing also publish an Authorised Professional Practice for Investigation which provides guidance on the key roles and principles on the process of criminal investigation. It includes guidance for both reactive and proactive investigations, from volume crime to major crime which can be found [here](#).

It clearly states within this APP that when working with victims the success of any investigation depends largely on the accuracy and detail of the material obtained from them. Although questions submitted for this request are statistical, confirmation or denial to the world that any information is held would undermine the confidentiality expected by a victim who reports to the police that they have been the subject to a crime or threat and have reported this to police under the auspices of Operation Bridger. Further information can be found [here](#).

Confirmation or denial that any further information is held relevant to this request would undermine both the APP for Intelligence Management and Investigations. The impact of confirming or denying whether information is held relating to this request, i.e. whether any incidents have been recorded under Op Bridger by a force to the NPCC has potential to undermine the flow of information (intelligence) by Police Service relating to allegations of crime. It also would undermine the tactical purpose of the operation, by highlighting to an offender whether their activities had been reported to the police thus hindering law enforcement.

Legislation - Section 30 Investigations and proceedings conducted by public authorities

(3) The duty to confirm or deny does not arise in relation to information which is (or if it were held by the public authority would be) exempt information by virtue of subsection (1) or (2).

Confirming or denying whether information exists relevant to this request would lead to a better informed general public by identifying that forces robustly investigate crimes against Members of Parliament. This fact alone may encourage individuals to provide intelligence in order to assist with investigations and promote public trust in providing transparency and demonstrating openness and accountability into where the police are currently focusing their investigations.

The security of Members of Parliament is a high profile topic, largely in part due to the tragic murders of Jo Cox and David Amess. Confirmation or denial that any information exists could provide reassurance to the general public.

However, by its very nature, information relating to the safety of individuals is highly sensitive. Under the Freedom of Information legislation, there is a requirement to comply with Section 1(1)(a) and confirm what information is held. In some cases it is that confirmation, or not, which could disclose facts which would undermine the investigative process and in such cases the NPCC takes advantage of its ability under FOI legislation to, where appropriate, neither confirm nor deny that information requested is or is not held.

Irrespective of what information is or isn't held, any information which could be used to undermine prosecutions or aid offenders is not in the public interest.

Legislation - Section 31 Law Enforcement

There is media speculation and rumour within the public domain relating to the security of Members of Parliament and that in itself can be considered to be a factor for disclosure.

The NPCC has a duty of care to the community at large, which obviously includes Members of Parliament. Public safety is of paramount importance. If an FOI disclosure revealed information to the world (by citing an exemption or stating no information held) that would undermine an operation and place the safety of an individual at risk, this could be used to an offenders advantage which would compromise public safety, the safety of Members of Parliament and it may also encourage offenders to carry out further crimes.

Irrespective of what information is or isn't held, applying substantive exemptions would indicate that information is held and has been/is currently being investigated. Such action would act as a deterrent to individuals provide intelligence to the force which would further undermine public safety, with repercussions that could hinder the prevention or detection of crime.

The NPCC would not wish to reveal who, what and when intelligence is recorded to individual forces and the extent of their investigations as this would clearly undermine the law enforcement and investigative process and allow criminals to plan their activity to better try to evade detection. This would impact on police resources and more crime and terrorist incidents would be committed, placing individuals at risk.

Confirmation or denial that information is held may hinder and undermine the partnership approach to law enforcement in this complex area.

In order for NCND exemptions to be effective, the NPCC considers that it is necessary to respond consistently to requests for certain types of information, both when the information is held and when it is not, without indicating whether or not the requested information is held.

As a result of the need for consistency, there is an inevitable degree of generality when explaining why the NPCC considers that it is exempt from the duty to confirm or deny in relation to certain types of requests.

The use of NCND in a consistent manner is recognised in the ICO guidance which states 'It can be important to use a neither confirm nor deny response consistently, every time a certain type of information is requested, regardless of whether the information is actually held or not. For this reason public authorities need to be alert to the possibility of receiving future requests for the same type of information when handling very specific or detailed requests.'

This consistent approach is further commented upon by the ICO who states, 'There are situations where a public authority will need to use the neither confirm nor deny response consistently over a series of separate requests, regardless of whether it holds the requested information. This is to prevent refusing to confirm or deny being taken as an indication of whether information is held. Before complying with section 1(1) (a), public authorities should consider both whether any harm would arise from confirming that information is held and whether harm would arise from stating that no information is held. Otherwise, if the same (or same type of)

requests were made on several occasions, a changing response could reveal whether information was held.'

The review is further guided by the ICO who states 'for many requests that public authorities receive, their decision to use a neither confirm nor deny response won't be affected by whether they do or don't in fact hold the information. The starting point and main focus in most cases will be theoretical considerations about the consequences of confirming or denying that a particular type of information is held.'

The ICO further reminds public authorities that they can only refuse to confirm or deny whether it holds the information, *'if this would itself reveal information that falls under an exemption'*.

To confirm that information is held by way of a FOIA disclosure must be considered as an acknowledgement to the world as a whole. Whilst it could be argued that it would be in the public interest to inform the public that the NPCC had an interest in particular individuals, groups or organisations, there are many factors which indicate that it is not in the public interest to acknowledge the existence or otherwise of such information in instances such as this.

To confirm or deny whether or not information is held, would clearly indicate the nature and scale of police involvement in the area of preventing and detecting crime.

In line with ICO guidance, as mentioned, the NPCC considers there to be the need to use the NCND response consistently over a series of separate requests, regardless of whether it holds the requested information. This is to prevent refusing to confirm or deny being taken by requesters as an indication of whether or not information is, in fact, held.

From previous ICO decision notices it can be seen that it is sufficient to demonstrate that either a hypothetical confirmation, or a denial, would engage the exemption. As such, it is not necessary to show that both confirming and denying information is held would engage the exemption from complying with section 1(1)(a) of the FOIA.

The ICO's guidance on the duty to confirm or deny further states:

'The wording of the request for information will affect whether or not a public authority will confirm or deny it holds that information. In many cases the more specific the request, the lower the likelihood of the duty arising.'

Your request specifically asked for information that, if held, would relate to policing investigation/s.

As such, this increases the harm that would be caused by confirming or denying whether information is held in relation to this request.

The points above highlight the merits of confirming, or denying, whether any information pertinent to this request 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, various intelligence may or may not be being handled. The Police Service will never divulge whether or not information pertinent to this request does or does not exist, if to do so would place the safety of an individual at risk, compromise an ongoing investigation or undermine the policing purpose in the effective delivery of operational law enforcement.

Whilst there is a public interest in the transparency of policing operations and investigations, providing reassurance that the Police Service is appropriately and effectively engaging with the threat from criminals,

there is a very strong public interest in safeguarding the health and safety of individuals. As much as there is a public interest in knowing that policing activity is appropriate and balanced it will only be overridden in exceptional circumstances.

Therefore, at this moment in time, it is our opinion that for these issues the balance test for confirming, nor denying that information is held is appropriate.

No inference can be taken from this refusal that information does or does not exist.

Legislation - Section 40(5A)& 40(5B) of the Act provides:

(5A) The duty to confirm or deny does not arise in relation to information which is (or if it were held by the public authority would be) exempt information by virtue of subsection (1).

(5B) The duty to confirm or deny does not arise in relation to other information if or to the extent that any of the following applies –

- (a) Giving a member of the public the confirmation or denial that would have to be given to comply with section 1(1)(a) – (i) would (apart from this Act) contravene any of the data protection principles.

These sections exempt personal information from disclosure if that information relates to someone other than the applicant, and if disclosure would reveal information about an individual or individuals, thereby breaching the right to privacy afforded to persons under the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR).

The NPCC considers that confirmation or denial that the information is held captured by this request is likely to breach the first data protection principle, which provides that personal data must be processed lawfully, fairly, and in a transparent manner. Disclosure would not constitute lawful and fair processing of the personal data because the individuals effected would not reasonably expect their identifiable information to be disclosed in relation to this request for information.