Met HQ Strategy & Governance
Information Law & Security Group
Information Rights Unit
PO Box 57192
London
SW6 1TR

Telephone: 0207 161 3500
Facsimile: 0207 161 3503
Email: foi@met.police.uk

www.met.police.uk

Your ref:
Our ref: 2016100001003

27 April 2017

Dear Mr Lamb

Freedom of Information Internal Review Reference No: 2016100001003

I write in connection with your correspondence dated 22/10/2016 in which you requested an internal review in relation to your request for information (ref: 2016080000763). The requested information was as follows:

> **'Under the terms of the Freedom of Information Act 2000, I ask for disclosure of information on whether a police investigation has begun to determine whether former Prime Minister Tony Blair committed the common law criminal offence of misconduct in public office over decisions he took which resulted in the military invasion of Iraq on 20 March 2003 by British forces. If an investigation has not already started, will an investigation be mounted using evidence from the Chilcot Report and from any other relevant sources?'**

DECISION

The Metropolitan Police Service (MPS) has completed its review and has decided to:

- Uphold the original decision

The MPS is not required to confirm or deny whether the requested information is held due to the following provisions of the Freedom of Information Act 2000 (FoIA):

- Section 17(1) - Refusal Notice
- Section 30(3) - Investigations and proceedings conducted by public authorities
- Section 40(5) - Personal Information

This is due to:

- the wording of the request, which is predicated upon the MPS confirming or denying the existence of a specific investigation; and
- the need for consistency when neither confirming nor denying whether information is held so as to protect policing information and personal data.

REASON FOR DECISION

Please see the legal annex for the sections of the Freedom of Information Act 2000 that are referred to in this letter and Appendix A attached for further information regarding the duty to confirm or deny.

The Freedom of Information Act 2000 creates a statutory right of access to information held by public authorities. Section 1(1) of the Act requires a public authority in receipt of a request to:

- Confirm whether they hold the requested information and if so,
- Communicate the requested information to the applicant.

Furthermore, the Freedom of Information Act is designed to place information into the public domain. Therefore, once access to information is granted to one person under the Act, it is then considered to be public information and must be communicated to any individual upon request. In accordance with this principle, the MPS routinely publishes information disclosed under the Freedom of Information Act on the MPS Internet site[1].

The right of access to information is subject to a number of exemptions that are designed to enable information that is not suitable for release to be withheld.

<u>The duty to confirm or deny</u>

The Information Commissioner's Office (ICO) guidance titled 'When to refuse to confirm or deny information is held' states[2]:

> *'In certain circumstances, even confirming or denying that requested information is held can reveal information that falls under an exemption. A public authority may be able to use an exemption to refuse to confirm whether or not it holds information, if either confirming or denying would reveal exempt information in itself.*
>
> *A neither confirm nor deny response is more likely to be needed for very specific requests than for more general or wide ranging requests.*
>
> *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.'*

[1] http://www.met.police.uk/foi/disclosure/disclosure_log.htm
[2] https://ico.org.uk/media/for-organisations/documents/1166/when_to_refuse_to_confirm_or_deny_section_1_foia.pdf

'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 ICO's guidance further explains the harm in issuing a statement confirming or denying whether information is held and demonstrates the following:

- Exempt information may be revealed by:
    - Confirming information is held
    - Confirming information is not held
    - Inconsistently applying neither confirm nor deny (NCND) exemptions in response to the same or similar requests
- It is only necessary to demonstrate the harm in one of the above scenarios for an NCND response to be appropriate
- Cumulative prejudice may result from multiple disclosures
- It would be sufficient for a public authority to demonstrate that a confirmation or denial would be revealing to someone with specialist knowledge
- The wording of a request may determine whether an NCND response is appropriate.

The ICO guidance also states:

'The exact wording of the request for information is an important consideration when deciding whether a public authority should confirm or deny if it holds the requested information. The more specific the request, the more likely it is that a public authority will need to give a neither confirm nor deny response.'

The MPS needs to be alert to requests for certain types of information, such as requests relating to investigations that may have been conducted.

The MPS regularly receives requests for information that, if held, could relate to investigations, infer personal data and/or otherwise relate to law enforcement. A hypothetical confirmation that such information is not held could also engage one or more FoIA exemptions.

Your queries are predicated upon the MPS confirming or denying whether an investigation has commenced in relation to an identifiable individual.

In relation to your request dated 18/08/2016, you were advised that the Metropolitan Police Service can neither confirm nor deny whether the information you requested was held.

Please find attached 'Appendix A' for further guidance in relation to the duty to confirm or deny.

Section 30 (Investigations and proceedings)

Section 30 is a 'class-based' exemption and would apply to any 'class' of information that would, if held, have been held at any time by the MPS for the purpose of an investigation the MPS has a duty to conduct. The harm in disclosing information relating to an investigation is inherent in the exemption.

The ICO guidance titled 'Investigations and proceedings (section 30)'[3] states:

> *'In broad terms, the section 30 exemptions exist to ensure the effective investigation and prosecution of offences and the protection of confidential sources. They recognise the need to prevent disclosures that would prejudice either a particular investigation or set of proceedings, or the investigatory and prosecution processes generally, including any prejudice to future investigations and proceedings.'*

The ICO's guidance titled Law Enforcement (Section 31)[4] states:

> *'83…**Typically, where a request identifies an individual or an organisation as the possible subject of an investigation or a particular line of enquiry a public authority could be pursuing, the more chance there is that confirming the information's existence would, or would be likely to, prejudice that investigation.***
>
> *84. Clearly confirming there was, or had been, an investigation would not be prejudicial if there had already been official acknowledgement of its existence.*
>
> *85. The example above demonstrates the need, in some circumstances, to apply the NCND provision consistently. **Where confirmation or denial would reveal whether a particular person was under investigation and where this would, or would be likely to, prejudice such investigations, public authorities should be alert to the need to apply the NCND provision. If it is only applied where the requested information is held, this will become apparent over time and defeat the purpose behind the exemption.**' [Emphasis added]*

The MPS has a duty to conduct investigations with a view to ascertaining whether a person should be charged with an offence, or whether a person charged with an offence is guilty of it. Consequently the MPS as a public authority is entitled to rely upon section 30(3) to the extent that the requested information, if held, could have been held at any time for the purpose of such investigations. As outlined above, it is necessary to use NCND exemptions consistently, regardless of whether the requested information is held or not. Consequently, citing section 30(3) in no way confirms or denies the existence of an investigation.

The table below displays the time periods within which exemptions relating to investigations and law enforcement can be applied to information requested under the Freedom of Information Act 2000.

---

[3] https://ico.org.uk/media/for-organisations/documents/1205/investigations-and-proceedings-foi-section-30.pdf
[4] https://ico.org.uk/media/for-organisations/documents/1207/law-enforcement-foi-section-31.pdf

Exemption	Applicable time period[5]
Section 30(1)	Was 30 years. Now 20 years (subject to transitional provisions)
Section 30(2)	No time limit
Section 31	100 years

These time periods could be seen as indicative of the time periods in which information can realistically prejudice investigations and law enforcement.

It is also pertinent to note that even when investigations and proceedings appear to have been concluded or closed, there is often a realistic possibility of:

- an investigation being reopened e.g. to investigate new lines of enquiry or review existing evidence
- the scope of an investigation being broadened or narrowed
- new investigations being carried out that relate to, or overlap with earlier enquiries.

The publication of the Chilcot report in July 2016 and the military invasion of Iraq in March 2003 suggests that a confirmation or denial statement in response to your request would relate to a relatively recent time period.

Your complaint correspondence dated 22/10/2016 indicated that your request related to misconduct in a public office and made no reference to 'war crimes'. With this in mind, it is pertinent to note that Section 30(3) is engaged because the wording of your request asks for a confirmation or denial as to whether or not an investigation has taken place. Therefore, the same rationale would broadly apply to the request regardless of any offences specified in the request.

In the circumstances of your request, the MPS is not required to confirm or deny whether the requested information is held.

[5] Section 62 and 63(1) of the Freedom of Information Act states:
62(1) For the purposes of this Part, a record becomes a "historical record" at the end of the period of **thirty years** beginning with the year following that in which it was created.
62(2) Where records created at different dates are for administrative purposes kept together in one file or other assembly, all the records in that file or other assembly are to be treated for the purposes of this Part as having been created when the latest of those records was created.
62(3) In this Part "year" means a calendar year.
63(1) Information contained in a historical record cannot be exempt information by virtue of section 28, **30(1)**, 32, 33, 35, or 42'
Section 63(4) of the Freedom of Information Act 2000 prohibits section 31, relating to law enforcement, from being applied to records created more than **100 years** ago.
http://www.legislation.gov.uk/ukpga/2000/36/part/VI
Schedule 7(4) of the Constitutional Reform and Governance Act 2010 amends section 62 of the Freedom of Information Act 2000 so that the definition of an historical record has been reduced to **20 years** subject to transitional provisions.
http://www.legislation.gov.uk/ukpga/2010/25/schedule/7

Section 40 – Personal Data

Section 40(5)(b)(i) of the Freedom of Information Act 2000 is applicable in circumstances where a confirmation or denial in relation to whether information is held would breach one or more of the data protection principles specified within the Data Protection Act 1998.

Personal data is defined within section 1 of the Data Protection Act 1998 as:

> *'data which relate to a living individual who can be identified—*
> *(a) from those data, or*
> *(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller'*

The ICO's guidance titled 'Determining what is personal data'[6] states:

> *"When considering identifiability it should be assumed that you are not looking just at the means reasonably likely to be used by the ordinary man in the street, but also the means that are likely to be used by a determined person with a particular reason to want to identify individuals. Examples would include investigative journalists, estranged partners, stalkers, or industrial spies."*

The ICO guidance titled 'Anonymisation: managing data protection risk code of practice'[7] states:

> *'Note that 'identified' does not necessarily mean 'named'. It can be enough to be able to establish a reliable connection between particular information and a known individual.'*

This shows that it is necessary to consider information that is in the public domain and/or information that may be known to other members of the public when considering whether individuals are identifiable.

Section 2 of the Data Protection Act also defines certain classes of information as 'sensitive personal data'. This includes information relating to:

- the racial or ethnic origin of the data subject
- political opinions
- religious beliefs or other beliefs of a similar nature
- membership of a trade union
- the physical or mental health or condition of an individual
- sexual life
- the commission or alleged commission of any offence
- any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

In considering whether confirming or denying whether or not the information requested is held would be in breach of any of the Data Protection Principles, the 1st

[6] https://ico.org.uk/media/for-organisations/documents/1554/determining-what-is-personal-data.pdf
[7] https://ico.org.uk/media/1061/anonymisation-code.pdf

data protection principle relating to 'fair and lawful processing' is relevant which states:

> *'1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—*
> *(a) at least one of the conditions in Schedule 2, and*
> *(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.'*

In the circumstances of your request, a confirmation or denial statement would clearly relate to an identifiable living individual (i.e. Tony Blair). Due to the law enforcement remit of the MPS, inferences could be made in relation to the commission or alleged commission of an offence which would constitute sensitive personal data. Furthermore, a confirmation or denial statement could also disclose or infer information relating to sources or alleged sources of information that may identifiable and/or constitute personal data.

The ICO guidance titled 'Personal information'[8] indicates that the following factors are relevant when assessing whether a disclosure under FoIA would be fair:

- whether the information is sensitive personal data;
- the possible consequences of disclosure on the individual;
- the reasonable expectations of the individual, taking into account:
    - their expectations both at the time the information was collected and at the time of the request
    - the nature of the information itself
    - the circumstances in which the information was obtained
    - whether the information has been or remains in the public domain
    - the FOIA principles of transparency and accountability
- any legitimate interests in the public having access to the information and the balance between these and the rights and freedoms of the individuals who are the data subjects.

<u>Section 40 – Sensitive personal data</u>

The ICO's guide to data protection[9] states the following in relation to personal data:

> *'The presumption is that, because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data.'*

A statement confirming or denying whether information has been received by the MPS in relation to a living individual, could constitute sensitive personal data as such information, due to the remit of the MPS may relate to:

- the commission or alleged commission of any offence

---

[8] http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Freedom_of_Information/Detailed_specialist_guides/personal-information-section-40-and-regulation-13-foia-and-eir-guidance.pdf

[9] https://ico.org.uk/media/for-organisations/guide-to-data-protection-2-2.pdf

- any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

Section 40 – Consequences of disclosure

A hypothetical confirmation or denial, or a pattern of such statements in response to similar requests, could disclose or infer personal data. This could cause unwarranted harm to the interests of individuals.

Depending upon the circumstances of a request the potential consequences of disclosure may vary. Based upon the wording of your request, a confirmation or denial statement could disclose or infer to the world at large whether one or more individuals have been the subject of an investigation. This may constitute and/or infer sensitive personal data. Disclosure of this type of information, if held, is likely to have a detrimental or distressing effect on the data subjects as sensitive personal data is, by its very nature, information that individuals regard as the most private information about themselves.

The ICO code of practice titled 'Anonymisation: Managing Data Protection Risk'[10] states:

> *'It is also generally unfeasible to see data return (ie recalling data or removing it from a website) as a safeguard given the difficulty, or impossibility, of securing the deletion or removal of data once it has been published.'*

Consequently, any harm in disclosure (i.e. a confirmation or denial statement) may be compounded by the information remaining in the public domain for a substantial length of time.

Due to the need for consistency when applying exemptions relating to the duty to confirm or deny, a confirmation or denial statement would also impair the ability of the MPS to protect personal data in response to similar requests which may have further consequences for the privacy of individuals.

Section 40 – Reasonable expectations

Individuals may have a reasonable expectation of confidentiality in relation to personal data held by the MPS or other law enforcement organisations. Information relating to the commission or alleged commission of an offence is classed as sensitive personal data and would reasonably carry an increased expectation of privacy.

The 2nd data protection principle states that:

> *'Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.'*

[10] https://ico.org.uk/media/1061/anonymisation-code.pdf

The purposes for which the MPS uses personal data are stated within the MPS Fair Processing Notice[11]. Section 1 of this document outlines 2 broad purposes for which the MPS obtains, holds, uses and discloses personal data as follows:

- *The Policing Purpose - which includes the prevention and detection of crime; apprehension and prosecution of offenders; protecting life and property; Preserving order; maintenance of law and order; rendering assistance to the public in accordance with force policies and procedures; National security; defending civil proceedings and any duty or responsibility of the police arising from common or statute law.*
- *The provision of services to support the Policing Purpose*

The MPS Data Protection Act 1998 (DPA) Compliance Standard Operating Procedures (SOP), published on the MPS Publication Scheme also outlines the way in which personal data held by the MPS should be handled. Section 8.6 of the SOP, titled 'How to ensure that the processing is lawful' also refers to the Code of Practice on the Management of Police Information (MoPI) which defines police information as:

- Protecting life and property;
- Preserving order;
- Preventing the commission of offences;
- Bringing offenders to justice; and
- Any duty or responsibility arising from common or statute law.

Individuals have the right to respect for their private and family life under Article 8 of the Human Rights Act 1998, which states:

> *1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'*

The MPS may also have a common law duty of confidentiality in relation to information that may be held regarding 3rd parties. The Ministry of Justice publication titled 'Public Sector Data Sharing: Guidance on the Law'[12] states:

> *'4. A duty of confidence arises whenever the party subject to the duty is in a situation where he either knew or ought to have known that the other person could reasonably expect his privacy to be protected. The disclosure of data may amount to a breach of confidence if all the following conditions are met:*
>
> - *The information in question has the necessary 'quality of confidence'. This means that the information should not be in the public domain or readily*

[11] http://www.met.police.uk/foi/pdfs/other_information/corporate/mps_fair_processing_notice.pdf
[12] http://webarchive.nationalarchives.gov.uk/20150730125042/http://www.justice.gov.uk/downloads/information-access-rights/data-sharing/annex-h-data-sharing.pdf

available from another source and that it should have a degree of sensitivity and value;

- *The information in question was communicated in circumstances giving rise to an obligation of confidence. The obligation of confidence may be express or implied from the circumstances, such as where there is a special relationship between professionals (for example, relationships between doctors and bankers and their clients). But there is no requirement for a prior relationship to exist between parties, and third parties can also be bound by the duty; and*
- *There was an unauthorised disclosure of that material.'*

Therefore, it would be reasonable for an individual to expect that any information that the MPS holds in relation to them, especially sensitive personal data, would only be used to support a policing purpose and not be unlawfully disclosed to 3rd parties.

The 7th data protection principle, specified within schedule 1 of the Data Protection Act 1998 states:

> *'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.'*

Consequently, the MPS have a legal obligation to take appropriate steps to protect personal data. In relation to personal data, one such organisational measure is to neither confirm nor deny whether personal data is held in certain circumstances.

Your complaint correspondence dated 22/10/2016 suggested that consideration should be given to disclosure in relation to the 'Prime Minister' not explicitly for a named individual. Notwithstanding the fact that the wording of your request names Tony Blair, any information relating to the 'Prime Minister' would clearly 'relate' to an identifiable individual in the context of your request and therefore constitute personal data.

A Prime Minister or former Prime Minister may have a reduced expectation of confidentiality due to the seniority and public facing nature of their role, especially in relation to decisions taken as part of their public role. However, the offence of misconduct in a public office would relate to individuals in a private capacity.

The MPS Media Policy Toolkit[13] states:

> ***'3. When do we confirm a police investigation or police activity and what information do we release?***
>
> *The nature of policing an investigation means it is hard to give a one-size-fits-all answer. However, there are general principles which should be followed as decisions on information release are made.*
>
> *…In the same way in which we deal with reactively responding to questions about individuals arrested, we would not identify individuals who are or may be*

[13] http://www.met.police.uk/foi/pdfs/disclosure_2015/august_2015/2015080000422.pdf

involved in an investigation and would not reactively respond in a way that would identify such individuals.'

'12. Does the MPS name people who have been arrested but not charged?

The current MPS policy is that people who have been arrested are not named by police unless there are exceptional circumstances. This is in line with Lord Justice Leveson's advice that save in exceptional circumstances the names or identifying details of those who are arrested or suspected of a crime should not be released.'*

A recent report by the House of Commons Procedure Committee titled 'Notification of the arrest of members'[14] summarises the MPS position in relation to the naming of individuals arrested where it states:

'17. … Identifying data about the investigation of an offence prior to the public action of charging is considered 'sensitive personal data' under the terms of the Data Protection Act 1998, and therefore may not be disclosed by a public authority. Police forces, when issuing statements confirming the arrest of individuals on suspicion of criminal offences, do not therefore give out the name of any arrested individual as a matter of course: statements made by police forces will customarily use a formulation such as 'a 48 year old male' to confirm that an arrest has been made. This safeguards the right to privacy of an individual up to the point when any charges may be brought.'

18. While the charging of an individual with a criminal offence is a public act and the name of the individual, and the offence with which he or she is charged, will be in the public domain, recent cases of media treatment of individuals said to be under investigation for notorious offences have highlighted the risks both to the effective conduct of justice and of violation of the right to privacy from the publication of names of arrested individuals before charge. The Law Commission has been consulting on issues relating to contempt of court in reporting of criminal cases. The Home Secretary, in recent guidance to the College of Policing, has set out her view that the arrest of an individual should only be made public in exceptional circumstances.

19. As the Clerk pointed out to us, police forces "inevitably" arrest people who turn out to be innocent of any wrongdoing. Arrests may also take place under a voluntary arrangement between the individual and the police…arrest is not now invariably followed by detention until charge, and arrested individuals may be released on bail to attend a police station at a later date.

20. The practice of the House in extending the requirement of notification of arrest to include the publication in the Votes and Proceedings of the name of an arrested Member, and therefore providing for the publication of details of the arrest, can have an unnecessary and avoidable impact on the privacy and the reputation of a Member where no charge follows. There are instances where the arrest of a Member has taken place in public, following participation

[14] https://www.publications.parliament.uk/pa/cm201516/cmselect/cmproced/649/649.pdf

in a demonstration or following instances of affray. Those are events which have taken place in the public eye and have inevitably attracted press attention. Members arrested on other criminal charges have chosen themselves to make the fact of their arrest public: and any Member may choose to disclose the fact of their arrest, as might any other member of the public.'

Although the above quote relates to the naming of members of parliament upon arrest, it is important to note that your request relates to whether or not an investigation has been conducted. If it would be unfair or unusual to name individuals upon arrest, it is likely to be more unfair or unexpected for the MPS to name individuals who are subject to an investigation prior to an arrest or charging decision being made. It is also pertinent to note that Tony Blair is no longer a member of parliament, albeit a former Prime Minister.

It is legitimate for the MPS to consider the effect of a confirmation or denial statement in the context of requests of a similar nature that may be received by the MPS at a later date. Such a statement may disclose personal data and/or impair the ability of the MPS to protect personal data relation to similar requests for information by undermining the use of NCND exemptions in the future. This is due to the information that would be disclosed by such a statement and/or a pattern of such statements.

Section 40 – Legitimate interests

The MPS recognises that there may be a legitimate public interest in confirming or denying whether the information requested is held. A legitimate interest is inherent in the disclosure of information upon request under the Freedom of Information Act given the associated benefit of enhancing the transparency and accountability of public authorities.

There may also be a legitimate public interest to the extent that the accountability and transparency of the MPS and police officers would be enhanced in relation to:

- actions
- investigations
- decisions
- the spending of public funds.

A confirmation or denial statement may also improve the quality of public debate regarding related issues of international importance and interest. This may also enhance public confidence.

Your complaint correspondence suggests that that Israelis coming to the UK are concerned about being arrested.

However, it is possible to meet the legitimate public interest identified above without confirming or denying whether or not the information requested is held.

For example, MPS finances, actions and decisions are also subject to external scrutiny by a number of organisations such as:

- Her Majesty's Inspectorate of Constabularies (HMIC).
- The Houses of Parliament

- The Independent Police Complaints Commission (IPCC)
- The Information Commissioner's Office (ICO).
- The Mayor's Office for Policing and Crime (MOPAC),
- The National Audit Office

Individuals may also choose to request information relating to themselves under the subject access provisions of the Data Protection Act 1998.

The Courts have their own rules permitting disclosure for the purpose of legal proceedings. For example, it may be possible to obtain a court order in relation to the disclosure of information.

This will usually mean that the disclosure of to the whole world under FOIA is not necessary.

The MPS also issue press releases and appeals for information where to do so would aid an investigation as demonstrated in the MPS Media Policy Toolkit[15] which states:

> ***'3. When do we confirm a police investigation or police activity and what information do we release?***
>
> *The nature of policing an investigation means it is hard to give a one-size-fits-all answer. However, there are general principles which should be followed as decisions on information release are made.*
>
> *The Media Policy's over-riding principle is - that we should be as open and transparent as possible, whilst ensuring operations, investigations, prosecutions, tactics and techniques and the safety of the public are not compromised and confidential information, including that concerning victims, witnesses and suspects is appropriately protected.*
>
> *We will proactively release information to aid an investigation - most likely with appeal points asking for the public's assistance. Information on investigations will also be proactively released when it is deemed to be a matter of public interest and there is a need to maintain public confidence in our policing activity.*
>
> *When the media ask questions about investigations or police activity, our principle is that we will reactively respond with information except where it will have a detrimental impact on the investigation or activity.'*

The ICO's guidance in relation to personal information further states:

> *'Although assessing fairness involves balancing the rights of data subjects against the legitimate interests in disclosure, this is not the same as carrying out the public interest test for qualified exemptions in FOIA…In particular,* ***there is no assumption of disclosure*** *as there is with qualified exemptions. Personal data can only be disclosed if to do so would satisfy the DPA*

[15] http://www.met.police.uk/foi/pdfs/disclosure_2015/august_2015/2015080000422.pdf

principles. If the public authority discloses personal data in contravention of DPA principles, it is in breach of its duty as a data controller.' [Emphasis added]

Conclusion - Section 40(5)

Section 40 of the Freedom of Information Act 2000 is designed to address information that is covered by the Data Protection Act 1998. Under section 40(5)(b)(i), the MPS is not required to confirm whether information is held if the confirmation or denial could contravene any of the data protection principles.

In this instance, for the reasons outlined above and communicated to you in the initial MPS response to your request, I have concluded that confirming or denying whether or not the requested information is held could contravene the 1st data protection principle, relating to the fair and lawful processing of personal data. Furthermore, in the circumstances of your request, none of the conditions specified within Schedule 2 or Schedule 3 of the Data Protection Act would be met in relation to confirming or denying whether or not the information requested is held.

Either of the exemptions cited in response to your request (i.e. section 30(3) and 40(5)) would be sufficient on their own for the MPS to neither confirm nor deny whether the requested information is held.

Please note that the rationale presented above is in relation to the duty to confirm whether the information requested is held by the MPS. Therefore, this correspondence neither confirms nor denies that the MPS holds the information that you have requested.

Advice and Assistance

You may be interested in the following ICO decision notices that relate to FoIA requests where police forces have been asked a number of questions predicated upon confirming or denying the existence of an operation/investigation and or related details:

Decision Notice FS50509831 (relates to a request for documents relating to an alleged police operation targeting the applicant)
https://ico.org.uk/media/action-weve-taken/decision-notices/2014/944186/fs_50509831.pdf

Decision Notice FS50529928 (relates to a request for information as to whether a particular police investigation was taking place)
https://ico.org.uk/media/action-weve-taken/decision-notices/2014/983400/fs_50529928.pdf

I would like to take this opportunity to apologise for any inconvenience caused by the delay in responding to your request for an internal review. This was primarily due to the MPS currently experiencing a high volume of FoIA requests and complaints.

If you are dissatisfied with this FoIA internal review, you have the right to appeal the decision by contacting the Information Commissioner for a decision on whether your request has been dealt with in accordance with the requirements of the Act.

For information on how to contact to the Information Commissioner please visit their website at www.ico.org.uk. Alternatively, phone or write to:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Phone: 0303 123 1113

Yours sincerely

Brian Wilson
Information Law Advisor

LEGAL ANNEX

Section 1(1) (General right of access to information held by public authorities) of the Freedom of Information Act 2000 states:

(1) Any person making a request for information to a public authority is entitled—
(a) to be informed in writing by the public authority whether it holds information of the description specified in the request, and
(b) if that is the case, to have that information communicated to him.

http://www.legislation.gov.uk/ukpga/2000/36/section/1

Section 17(1) (Refusal of request) of the Freedom of Information Act 2000 states:

(1)A public authority which, in relation to any request for information, is to any extent relying on a claim that any provision of Part II relating to the duty to confirm or deny is relevant to the request or on a claim that information is exempt information must, within the time for complying with section 1(1), give the applicant a notice which—
(a) states that fact,
(b) specifies the exemption in question, and
(c) states (if that would not otherwise be apparent) why the exemption applies.

http://www.legislation.gov.uk/ukpga/2000/36/section/17

Section 30(1)(a), 30(2) & 30(3) (Investigations) of the Freedom of Information Act 2000 states:

(1) Information held by a public authority is exempt information if it has at any time been held by the authority for the purposes of-
(a) any investigation which the public authority has a duty to conduct with a view to it being ascertained-
(i) whether a person should be charged with an offence, or
(ii) whether a person charged with an offence is guilty of it

(2) Information held by a public authority is exempt information if—
(a) it was obtained or recorded by the authority for the purposes of its functions relating to—
(i) investigations falling within subsection (1)(a) or (b),
(ii) criminal proceedings which the authority has power to conduct,
(iii) investigations (other than investigations falling within subsection (1)(a) or (b)) which are conducted by the authority for any of the purposes specified in section 31(2) and either by virtue of Her Majesty's prerogative or by virtue of powers conferred by or under any enactment, or
(iv) civil proceedings which are brought by or on behalf of the authority and arise out of such investigations, and
(b) it relates to the obtaining of information from confidential sources.

(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).

http://www.legislation.gov.uk/ukpga/2000/36/section/30

Section 40(2), 40(3) & 40(5) (Personal Information) of the Freedom of Information Act 2000 states:

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

(3) The first condition is—
(a) in a case where the information falls within any of paragraphs (a) to (d) of the definition of "data" in section 1(1) of the Data Protection Act 1998, that the disclosure of the information to a member of the public otherwise than under this Act would contravene—
(i) any of the data protection principles, or

(5)The duty to confirm or deny—
(a) 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), and
(b) does not arise in relation to other information if or to the extent that either—
(i) the giving to a member of the public of the confirmation or denial that would have to be given to comply with section 1(1)(a) would (apart from this Act) contravene any of the data protection principles or section 10 of the Data Protection Act 1998 or would do so if the exemptions in section 33A(1) of that Act were disregarded, or
(ii) by virtue of any provision of Part IV of the Data Protection Act 1998 the information is exempt from section 7(1)(a) of that Act (data subject's right to be informed whether personal data being processed).

http://www.legislation.gov.uk/ukpga/2000/36/section/40