

|  |  |
| --- | --- |
|  | Information Rights UnitPO Box 313SidcupDA15 0HHEmail: foi@met.police.uk[www.met.police.uk](http://www.met.police.uk)Your ref: Our ref: 01/FOI/21/01902014/05/2021 |
|  |

Dear Ms. Smith

**Freedom of Information Review Reference No: 01/FOI/21/019020**

I am sorry you are disappointed with the outcome of your Freedom of Information Act (FOIA / the Act) request reference number 01/FOI/21/018441.

Further to our earlier correspondence, I am now able to provide a response to your request for an Internal Review of our decision.

**Background to your request for an Internal Review:**

This Internal Review concentrates on the following request that you submitted to the Metropolitan Police Service (MPS) on 14/03/2021:

*Please supply a copy of the Tactical Advice in relation to the Policing of the 'Vigil for Sarah' that took place on Clapham Common on the evening of 13th March 2021.*

*I do not require any information that identifies any individual person(s) and if any of the documents I request contain any identification of individual persons then please redact these details.*

On 16/04/2021, we refused your request by virtue of the following FOIA exemptions:

* Section 31(1)(a)(b) – Law enforcement
* Section 40(2) and 40(3A) (a) - Personal information.

On 17/04/2021, you requested an Internal Review. You wrote:

*I am writing to request an internal review of Metropolitan Police Service (MPS)'s handling of my FOI request 'Vigil for Sarah - Clapham Common - The evening 13th March 2021 - Tactical Advice'.*

*It would be proportionate to release the information requested and the exemptions you rely upon are not applicable in these circumstances.*

**Decision:**

The MPS has completed its Internal Review and has decided to uphold its decision.

**Reasons for Reliance on Section 31 Law Enforcement**

As part of the Review, I have assessed whether Section 31 exemption has been applied appropriately.

In order for the exemption provided under Section 31(1) to be engaged in this case, the MPS must show that disclosure under the Act would, or would be likely to, prejudice law enforcement functions, namely Section 31(1)(a) the prevention and detection of crime.

The ICO guidance points to the fact this exemption is a two-stage test. Firstly, can a public authority establish that disclosure of the information would prejudice, or would be likely to prejudice, any of the areas of law enforcement listed in section 31 (i.e. prevention or detection of crime). Secondly, if so, is the public interest in favour of maintaining the exemption and therefore withholding the information.

The ICO advises *‘although there must be a casual link, the prejudice test relates to something that may happen in the future, if the information were disclosed. Therefore it is not usually possible to provide concrete proof that the prejudice would or would be likely to result. Nevertheless…there must be more than a mere assertion or belief that disclosure would lead to prejudice. There must be a logical connection between the disclosure and the prejudice in order to engage the exemption.’* The review is further guided by the ICO who states *‘in considering the application of the exemption, a public authority should concentrate on the effect of disclosure in order to assess whether there is any likely prejudice to any law enforcement activities listed in the exemption. There is no need to consider why the information is held’*.

The Review also has regard for the same guidance in the general areas of law enforcement which states under the heading apprehending or prosecution of offenders *‘it could cover activities both in relation to specific instances of the apprehension and prosecution of offenders and to the general strategies, processes and policies established for these purposes…’*

You have asked for the tactical advice used by the MPS for the policing of the ‘Vigil for Sarah’. This request for information may seem harmless on its own given that the event is in the past, however we have to mindful of the effect of disclosure on policing tactics in general. Those with the necessary criminal intent, inclination and capacity could use the information to gain an operational advantage over the MPS as the information can be classed as operational 'intelligence' and operationally sensitive.

This information pieced together with other information in the public domain and / or gathered from other sources, may provide those seeking to cause harm with valuable intelligence regarding MPS tactical options and capabilities.

It would not be in the public interest to disclose the requested information as it is likely to impact on any similar future police operations. The MPS are likely to need to adapt their tactics and strategies if detailed information is disclosed concerning the processes, plans and tactics employed for this sort of matter.

FOIA disclosures are placed into the public domain and as mentioned, disclosures which appear innocuous, pieced together with other disclosures can be used in a ‘mosaic effect’ to give a fuller picture to those wishing to evade detection and valuable intelligence to criminals.

This ‘cumulative prejudice’ or the ‘mosaic effect’ whereby the information requested may be of increased significance when combined with other information obtained through other means and/or at a later date. The ‘mosaic’ effect has been described as follows:

*‘The “mosaic theory” describes a basic precept of intelligence gathering: Disparate items of information, though individually of limited or no utility to their possessor, can take on added significance when combined with other items of information. Combining the items illuminates their interrelationships and breeds analytic synergies, so that the resulting mosaic of information is worth more than the sum of its parts.’ -* Source: David Pozen, The Mosaic Theory, National Security, and the Freedom of Information Act, 115 Yale L. J. 628, 630 (2005).

The Information Commissioner’s guidance in relation to Law Enforcement acknowledges the harm that may be caused by the mosaic effect where it states:

*‘Mosaic and precedent effects*

*21. The prejudice test is not limited to the harm that could be caused by the requested information on its own. Account can be taken of any harm likely to arise if the requested information were put together with other information. This is commonly known as the ‘mosaic effect’. As explained in the Information Commissioner’s guidance information in the public domain, the mosaic effect usually considers the prejudice that would be caused if the requested information was combined with information already in the public domain.*

*22. However, some requests can set a precedent, ie complying with one request would make it more difficult to refuse requests for to refuse requests for similar information in the future. It is therefore appropriate to consider any harm that would be caused by combining the requested information with the information a public authority could be forced to subsequently provide if the current requested was complied with. This is known as the precedent effect.’*

Access to information is essential to democratic discourse and open and informed debate. The disclosure of information facilitates transparency and accountability and may increase citizens’ empowerment and participation in society. However, for the reasons explained above, the Review believes that the balance of the public interest in this instance favours exempting the information you have requested by virtue of Section 31 Law Enforcement as disclosure would likely prejudice the prevention or detection of crime. The Review considers that the public interest in this matter has been met by the bespoke thematic inspection conducted by Her Majesty’s Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) into the MPS’s handling of the event, its operational decision-making, application of the law in the context of the COVID regulations and its engagement with those at the vigil and the wider public.

**Reasons for reliance on Section 40 – Personal Information**

The exemption has been applied as disclosure of the information you have requested could identify living individuals linked to information collated for policing purposes. The exempted information constitutes personal data which would, if released, be in breach of the rights provided by the DPA (Data protection Act) 2018 and GDPR (General Data Protection Regulation).

Section 40(2) of the FOIA provides that information is exempt from disclosure if it is the personal data of an individual other than the requester and where one of the conditions listed in section 40(3A) (3B) or 40(4A) is satisfied.

In this case the relevant condition is contained in section 40(3A)(a). This applies where the disclosure of the information to any member of the public would contravene any of the principles relating to the processing of personal data as set out in Article 5 of the GDPR.

The first principle of the DPA provides that personal data must be processed lawfully and fairly. It states:

***The first data protection principle***

*(1) The first data protection principle is that the processing of personal data for any of the law enforcement purposes must be lawful and fair.*

*(2)The processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law and either—*

*(a)the data subject has given consent to the processing for that purpose, or*

*(b)the processing is necessary for the performance of a task carried out for that purpose by a competent authority.*

ICO guidance on employee personal data[[1]](#footnote-1) states:

*When a public authority receives a request for information that constitutes personal data about its employees, it must decide whether disclosure would breach Principle 1 of the Data Protection Act (the DPA), ie whether it would be fair and lawful to disclose the information.*

*Whether the disclosure is fair will depend on a number of factors including:*

*• whether it is sensitive personal data;*

*• the consequences of disclosure;*

*• the reasonable expectations of the employees; and*

*• whether there is a legitimate interest in the public or requester having access to the information and the balance between this and the rights and freedoms of the data subjects.*

*If the public authority decides that it would be fair, the disclosure must also satisfy one of the conditions in Schedule 2 of the DPA.*

*In addition, if the information constitutes sensitive personal data, the disclosure must also satisfy one of the conditions in Schedule 3 of the DPA.*

With respect to fairness and reasonable expectations, the Review takes due regard to the ICO guidance concerning these matters:

***Fairness***

*12. There are a number of factors that could indicate whether disclosure would be fair, including whether it is sensitive personal data, the consequences of disclosure, the employees’ reasonable expectations and the balance between their rights and the legitimate interests of the public and the requester in disclosure: Sensitive personal data*

*13. If the information is sensitive personal data, as defined in the DPA section 2, disclosure is unlikely to be fair. This data is likely to relate to the most personal aspects of employees’ lives, for example their health or sexual life, rather than their working life. Employees would have a reasonable expectation that this data would not be made public. Furthermore, such a disclosure would also have to meet a condition in both Schedule 2 and Schedule 3 of the DPA. Consequences of disclosure*

*14. Disclosure is unlikely to be fair if it would have unjustified adverse effects on the employees concerned. Although employees may regard the disclosure of personal information about them as an intrusion into their privacy, this may often not be a persuasive factor on its own, particularly if the information relates to their public role rather than their private life. If an authority wishes to claim that disclosure would be unfair because of the adverse consequences on the employees concerned, it must be able to put forward some justification for this claim.*

***Reasonable expectations***

*15. A key issue to consider in assessing fairness is whether employees have a reasonable expectation that their information will not be disclosed. This will depend on a number of factors, including:*

*• Whether the information relates to the employee in their professional role or to them as individuals*

*16. Information about an employee’s actions or decisions in carrying out their job is still personal data about that employee, but given the need for accountability and transparency about public authorities, there must be some expectation of disclosure. On the other hand, information that may be held in a personnel file about their health or disciplinary record or payroll information about their tax code all relate to them as individuals and to their personal circumstances and there is a greater expectation that a public authority would not disclose such information.*

The Review considers that those individuals whose names are contained within the requested information would not reasonably expect the MPS to put information in the public domain which identifies them. Such disclosure could lead to unwanted and unwarranted intrusion and distress.

**Conclusion:**

I hope the Review provides clarity why the MPS has reached the decisions detailed in this response.

If you are dissatisfied with the outcome of this Internal Review, you have the right to appeal the decision by contacting the Information Commissioner's Office (ICO) for a decision on whether the request for information has been dealt with in accordance with the requirements of the FOIA.

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

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Phone: 0303 123 1113

Yours sincerely

**Yvette Taylor**

**Information Manager**

1. https://ico.org.uk/media/for-organisations/documents/1187/section\_40\_requests\_for\_personal\_data\_about\_employees.pdf [↑](#footnote-ref-1)