



Ministry of Defence Police

MDP Secretariat
Room 126, Building 1070
MDP HQ Wethersfield
Braintree, Essex CM7 4AZ

Tel: 01371 85 [REDACTED]

E-mail: MDP-FOI-DP@mod.gov.uk

Our Ref: eCase: FOI 2018/12289 RFI:314/18

Date: 4 December 2018

[REDACTED]
[REDACTED]
Dear [REDACTED]

FREEDOM OF INFORMATION ACT 2000: MINISTRY OF DEFENCE POLICE: USE OF SOCIAL MEDIA AS AN INVESTIGATIVE TOOL

I refer to your email dated 4 October 2018 which was acknowledged on the same date.

I am treating your email as a request for information in accordance with the Freedom of Information Act 2000 (FOIA 2000).

In your email you requested the following information:

- 1. Does your police force use Facebook as an investigative tool? If yes, can you outline how eg for OSINT purposes, undercover work and/or evidence collection?**
- 2. What year did your police force start to use Facebook as an investigative tool?**
- 3. Does your police force use Twitter as an investigative tool? If yes, can you outline how eg for OSINT purposes, undercover work and/or evidence collection?**
- 4. What year did your police force start to use Twitter as an investigative tool?**
- 5. Are there any guidelines for how Twitter and Facebook should be used as an investigative tool eg for OSINT purposes, undercover work and/or to gather evidence of criminality that is admissible in court? If yes, what year were these guidelines published?**
- 6. Can I be provided with these guidelines both for OSINT, undercover work and evidence gathering collection via social media?**

A search for information has been completed by the Ministry of Defence Police (MDP) and I can confirm that we do hold information in scope of your request as follows:

1. Does your police force use Facebook as an investigative tool? If yes, can you outline how eg for OSINT purposes, undercover work and/or evidence collection?

Yes. In respect of “how” please see below.

2. What year did your police force start to use Facebook as an investigative tool?

Estimated as 2010

3. Does your police force use Twitter as an investigative tool? If yes, can you outline how eg for OSINT purposes, undercover work and/or evidence collection?

Yes. In respect of “how” please see below.

4. What year did your police force start to use Twitter as an investigative tool?

Estimated as 2010

5. Are there any guidelines for how Twitter and Facebook should be used as an investigative tool eg for OSINT purposes, undercover work and/or to gather evidence of criminality that is admissible in court? If yes, what year were these guidelines published?

The Ministry of Defence Police follow the NPCC guidance on Open Source Investigation/Research.

6. Can I be provided with these guidelines both for OSINT, undercover work and evidence gathering collection via social media?

This guidance is available online.

Information relating to the “how” element of your question 1 and 3 is withheld under Section 31(1)(a)(b) Law Enforcement, Section 31 is a prejudice based exemption. I have conducted a Public Interest Test and concluded that the balance favours exempting the information from release. Although transparency and openness are vital for promoting public confidence Section 31(1)(a)(b) applies because the release of information as to how both Facebook and Twitter are used for investigative purposes by the Ministry of Defence Police would place policing techniques in the public domain and undermine investigations.

Additionally the Ministry of Defence can neither confirm nor deny that they hold any other information relevant to your request by virtue of the following exemptions:

Section 23(5) – information relating to security bodies

Section 23 is a class based absolute exemption and not subject to a public interest test.

Section 31(3) – Law Enforcement

Section 31(3) is a prejudice based qualified exemption and there is a requirement to articulate the harm that would be caused by confirming or not that any information is held as well as carrying out a public interest test.

Section 31(3) is engaged because to confirm or deny whether the Ministry of Defence Police hold any additional information would mean that law enforcement tactics could be compromised which would hinder the prevention and detection of crime.

This should not be taken as conclusive evidence that any information that would meet your request does or does not exist.

If you wish to complain about the handling of your request, or the content of this response, you can request an independent internal review by contacting the Information Rights Compliance team, Ground Floor, MOD Main Building, Whitehall, SW1A 2HB (e-mail CIO-FOI-IR@mod.gov.uk).

Please note that any request for an internal review should be made within 40 working days of the date of this response.

If you remain dissatisfied following an internal review, you may raise your complaint directly to the Information Commissioner under the provisions of Section 50 of the Freedom of Information Act. Please note that the Information Commissioner will not normally investigate your case until the MOD internal review process has been completed. The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Further details of the role and powers of the Information Commissioner can be found on the Commissioner's website at <https://ico.org.uk/>.

Yours sincerely

MDP Secretariat and Freedom of Information Office