Department of Health & Social Care

Freedom of Information Team
Department of Health and Social Care
39 Victoria Street
London
SW1H 0EU

www.gov.uk/dhsc

Mr Don Priest
mailto:request-563075-2b605adb@whatdotheyknow.com

12 August 2019

Dear Mr Priest

Freedom of Information Request Reference FOI-1170888

Thank you for your request to the Department of Health and Social Care (DHSC) dated 19 March 2019, the full text of which is attached hereto. The questions you submitted as requests under the Freedom of Information Act (FOIA) are as follows:

Qu 1 What security rules, codes, protocols, procedures and precautions are taken to ensure that the CIA, GCHQ /Cabinet office are not eavesdropping / spying on staff, officials and ministers in your Department with social media media eg Google, Facebook as a conduit?

Qu 2 What summaries / reports does the department have about its cyber security? Please indicate the public facing reports.

Qu 3 Has the Department risk assessed the threat posed by social media, especially that owned by foreign corporations and countries and especially US and CIA? What summaries does the department have of this information, including any public facing ones?

Qu 4 What social media apps are allowed on the Departments phones and computers?

Which are installed?

Qu 5 Are Facebook, Google and Twitter apps allowed to be installed and or used on Department computers and mobile phones?

Qu 6 Are private, ie individually owned, mobile phones and computers with social media apps installed such as Facebook, Google and Twitter allowed in Department meetings, committees, and in the office environment?

Qu 7 If the answer to Qu 5 and Qu 6 are yes, how does the Department stop companies / CIA spying utilising microphones, cameras, and GPS data on those devices?

Qu 8 Has the department informed staff of the risk of spying and eavesdropping via social media apps? If so please send a copy of the memo / paper.

Qu 9 Has the Department contributed material to the Cabinet Office as part of the cyber security strategy? If so what?

Questions on Q sometimes written as QAnon, #Q #QAnon

(Background information on Q follows the questions)

Qu 10 Has the Secretary, Ministers or the top 3 civil servants in the Department been briefed about QAnon?

Qu 11 If so please indicate the date and the type of recorded information that has been briefed so that any future request may be narrowed down, as per Section 16 of the UK freedom of Information Act and Information Commissioner Guidance.

Qu 12 Has the Department any other recorded information on Q / QAnon ? If so please indicate the date and the type of recorded information that has been briefed so that any future request may be narrowed down, as per Section 16 of the UK freedom of Information Act and Information Commissioner Guidance. (If there is a mass of information that will take the request over the time limit, please disregard this question)

(Please note that the above includes the small change to the wording in Question 10 which you sent us an email about on 21 March).

Your request has been handled under the Freedom of Information Act (FOIA). With apologies for the delay in replying, our response to your questions is as follows.

Questions 1-7

Qu 1 What security rules, codes, protocols, procedures and precautions are taken to ensure that the CIA, GCHQ /Cabinet office are not eavesdropping / spying on staff, officials and ministers in your Department with social media media eg Google, Facebook as a conduit?

Qu 2 What summaries / reports does the department have about its cyber security? Please indicate the public facing reports.

Qu 3 Has the Department risk assessed the threat posed by social media, especially that owned by foreign corporations and countries and especially US and CIA? What summaries does the department have of this information, including any public facing ones?

Qu 4 What social media apps are allowed on the Departments phones and computers? Which are installed?

Qu 5 Are Facebook, Google and Twitter apps allowed to be installed and or used on Department computers and mobile phones?

Qu 6 Are private, ie individually owned, mobile phones and computers with social media apps installed such as Facebook, Google and Twitter allowed in Department meetings, committees, and in the office environment?

Qu 7 If the answer to Qu 5 and Qu 6 are yes, how does the Department stop companies / CIA spying utilising microphones, cameras, and GPS data on those devices?

I can neither confirm nor deny whether DHSC holds the information you have requested in Questions 1 to 7. Sections 24(2) and 31(3) of the FOIA, which relate to bodies dealing with national security and law enforcement, allow public authorities to neither confirm nor deny that requested information is held, if doing so would in itself disclose sensitive or potentially damaging information that falls under an exemption.

Section 24 (2) states that:

"The duty to confirm or deny does not arise if, or to the extent that, exemption from section 1(1)(a) is required for the purpose of safeguarding national security."

Section 31(3), Law Enforcement states that:
"The duty to confirm or deny does not arise if, or to the extent that compliance with section 1(1)(a) would or would be likely to, prejudice any of the matters mentioned in subsection (1)."

Sections 24 and 31 are qualified exemptions and DHSC has considered whether the public interest in maintaining the exemption of the duty to confirm or deny outweighs the public interest in confirming whether or not DHSC holds any information.

DHSC recognises that there is a general public interest in transparency in government as this increases public trust and engagement.

But this has to be weighed against a strong public interest in safeguarding national security and preventing and detecting crime. In this instance, confirming whether or not we hold information, may assist someone in planning effective cyber security attacks, and could compromise measures to protect government ICT systems leaving them vulnerable. The information could assist in criminal activity if the information was used by malicious parties to conduct future attacks. If ICT systems are attacked it could lead to the loss of confidentiality, integrity and availability of government information. In this case, we have decided that the public interest in maintaining the exclusion outweighs the public interest in confirming or denying whether the information is held.

Qu 8 Has the department informed staff of the risk of spying and eavesdropping via social media apps? If so please send a copy of the memo / paper.

DHSC does not hold this specific information. However, we do advise staff not to use social media for work purposes, and there is general Cabinet Office guidance on classification of government information.

Qu 9 Has the Department contributed material to the Cabinet Office as part of the cyber security strategy? If so what?

DHSC holds relevant information, and I can confirm that we are compliant with the Cabinet Office baseline security standards/ SPF.

Qu 10 Has the Secretary, Ministers or the top 3 civil servants in the Department been briefed about QAnon?

DHSC holds no relevant information.

Qu 11 If so please indicate the date and the type of recorded information that has been briefed so that any future request may be narrowed down, as per Section 16 of the UK freedom of Information Act and Information Commissioner Guidance.

DHSC holds no relevant information.

Qu 12 Has the Department any other recorded information on Q / QAnon ? If so please indicate the date and the type of recorded information that has been briefed so that any future request may be narrowed down, as per Section 16 of the UK freedom of Information Act and Information Commissioner Guidance. (If there is a mass of information that will take the request over the time limit, please disregard this question)

DHSC holds no relevant information.

If you are not satisfied with the handling of your request, you have the right to appeal by asking for an internal review. This should be submitted within two months of the date of receipt of the response to your original letter and should be addressed to the address at the top of this letter, or the email address at the end of this letter.

Please remember to quote the reference number above in any future communications.

If you are not content with the outcome of your internal review, you may complain directly to the Information Commissioner (ICO) who may decide to investigate your concerns. Generally, the ICO cannot make a decision unless you have already appealed our original response, and received our internal review response. The ICO will not usually investigate concerns where there has been an undue delay in bringing it to their attention. You should raise your concerns with them within three months of your last meaningful contact with us.

The ICO can be contacted at:

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

https://ico.org.uk/concerns/

Yours sincerely,

Dorothy Crowe

Freedom of Information Officer
E FreedomofInformation@dhsc.gov.uk