14 July 2020

FREEDOM OF INFORMATION (FOI) REQUEST

Thank you for your enquiry, received on 17 June 2020.

Specifically you requested:

1. What reseller do you prefer to buy your Software through?
2. Are there any favoured frameworks you tend to use?
3. Who is the decision-maker for IT Purchasing?
4. Who is your mobile phone provider?
5. What Mobile Device Management Solution are you using and when is the renewal date?
6. What Mobile Threat Detection do you have in place for mobile devices and when is the renewal date?
7. What Virtual Desktop Software do you have in place for remote workers and when is the renewal date?
8. Do you currently use a document security or digital rights management tool and when is the renewal date?
9. What are you using for instant messaging?
10. Who do you currently use for your Annual IT health checks and when is your next one due?
11. What email exchange server are you running? Cloud or on-premise?
12. What antivirus software/tool do you use and when is the renewal date?
13. Do you have an incident response team within your IT department?

Our response

1. The CCC utilises the Defta IT contract, Defra Group Commercial must follow public sector policy rules on procurement. All public procurement must be based on value for money, defined as "the best mix of quality and effectiveness for the least outlay over the period of use of the goods or services bought". This should be achieved through competition, unless there are compelling reasons to the contrary.

2. The CCC utilises the Defta IT contract, there are no favoured frameworks. Defra group Commercial (DgC) has access to a suite of frameworks, including but not limited to Crown Commercial Services, Digital Marketplace and other Government and Public Sector frameworks. The scope of the selected framework must meet the business need. Market analysis work is undertaken to determine the best route to market.

3. After careful consideration we have decided that details of the staff decision-makers should be withheld under sections 40(2) and 40(3A) of the FOIA as the information constitutes personal data relating to persons other than you. These sections exempt personal information from disclosure if that information relates to someone other than the applicant, and if disclosure of that information would breach any of the data protection principles in Article 5(1) of the General Data Protection Regulation (GDPR). We consider that disclosure of this information 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 'fair' processing of the personal data because the junior staff involved would not reasonably expect their contact details to be disclosed in relation to this request for information, and equally the senior members of staff would not reasonably expect their contact details to be disclosed in relation to this request.

4. Vodafone.

5. VMWare Workspace One MDM.

6. We use the secure MDM above and comply with all the iOS upgrades when they come out.

7. This information is being withheld under section 31(1)(a) of the FOIA. Please see the explanation below.

8. Yes, both, end date is Q2 2023.

9. Cisco Jabber and Microsoft Teams

10. This information is being withheld under section 31(1)(a) of the FOIA. Please see the explanation below.

11. Defra is in the process of moving its legacy on-premise email exchange servers to cloud Exchange Online. This migration has largely been completed apart from a small residual on-premise footprint still to be complete.

12. This information is being withheld under section 31(1)(a) of the FOIA. Please see the explanation below.

13. Yes, we have an IT incident management function which operates 24x7.

<u>Section 31(1)(a)</u>

The information that you have requested in questions 7, 10 and 12 of your request is being withheld as it falls under the exemption in section 31(1)(a) of the FOIA, which relates to the prevention or detection of crime. In applying this exemption, we have had to balance the public interest in disclosing the information, against the public interest in withholding it.

We recognise that there is a public interest in disclosure of information around IT health checks, antivirus software and IT software, as this will promote openness and transparency within Government, and also show whether the functions of Government are adequately protected from cyber-attacks.

However, there is a strong public interest in withholding details about health checks, cyber-security and IT software, as it could aid potential attackers by providing them with the information necessary to consider mounting a possible attack. Any attempt to carry out a cyber-attack against an IT system is a criminal offence. Providing information on cyber-attacks, cyber policies and cyber risks in the department, would assist someone in testing the effectiveness of Defra defences against such attacks and could also assist a criminal to deduce if their attacks had been detected or thwarted. This exemption is engaged because releasing the information will prejudice the prevention of crime by facilitating the possibility of a criminal offence being carried out. Releasing information which can be used to aid or plan a cyber-attack is withheld and we apply this rule across all government departments as it would have detrimental impacts to the running of public services.

We have therefore decided that the information should be withheld.

If you are dissatisfied with the handling of your request, you have the right to ask for an internal review. If you are not content with the outcome of the review, you may apply directly to the Information Commissioner for a decision.

In keeping with our transparency policy, the information released to you will be published on www.theccc.org.uk. Please note that this publication will not include your personal data.

Kind regards,

Committee on Climate Change