

Reference: 2026-063

Thank you for your email in which you requested the following information under the Freedom of Information Act 2000 (FOIA):

I would like answers to the questions below. For the purposes of this request, “temporary overseas working” means an employee who is ordinarily based in the UK being authorised to perform their normal duties remotely from another country. Please exclude official overseas postings, diplomatic postings and ordinary international business travel.

1) Does your department permit UK-based employees to work temporarily from locations outside the UK? If yes, please confirm whether employees are required to:

- a. Notify the department before working from outside the UK.**
- b. Obtain formal approval before working from outside the UK.**

2) At the date of this request, has your department approved any arrangements allowing UK-based employees to work temporarily from another country at any point between 1 May and 30 September 2026? If yes, please provide:

- a. The number of approved arrangements covering any part of this period.**
- b. A list of the destination countries covered by those approved arrangements.**

3) At the date of this request, please state whether each of the following controls/measures are in place for employees authorised to work temporarily overseas using departmental endpoints such as laptops, mobile phones or tablets. Please answer Yes, Partially, No, or Information not held for each control:

- Centralised mobile or unified endpoint management**
- Full-disk encryption on department-managed endpoint devices**
- Multi-factor authentication for access to departmental systems, applications or data from endpoint devices**
- Conditional-access controls that restrict access where a device does not meet the department’s security or compliance requirements**
- Ongoing identity assessment used to support a Zero Trust access model**
- Endpoint Detection and Response or Extended Detection and Response capabilities**
- Automated deployment of operating-system and application security patches to endpoint devices**
- Controls that restrict or adapt access according to the country or geographical location from which a user or device connects**
- Data-loss-prevention controls designed to prevent sensitive departmental data from being copied, downloaded, transferred or otherwise removed from managed endpoint devices without authorisation**
- The ability to remotely lock or erase a managed endpoint device**
- Continuous or scheduled monitoring of endpoint-device compliance with departmental security policies.**
- A requirement for employees working overseas to use a department-managed device rather than a personal device**

Response

Question 1a & b

Yes, the SFO permits UK-based employees to work temporarily from locations outside the UK. Employees are required to notify and obtain formal approval before working from outside the UK.

Question 2a & b

The SFO holds this information. However, we are withholding the specific number of approved arrangements and the list of destination countries under section 40(2) of the Freedom of Information Act 2000 (FOIA).

Section 40(2) provides that personal data relating to a third party is exempt from disclosure if releasing it would contravene the data protection principles. In this case, disclosure would breach the first data protection principle, which requires that personal data be processed lawfully, fairly and transparently.

How the exemption is engaged

The SFO is a relatively small organisation, and the number of staff working temporarily overseas during the requested period is very small. Disclosing the number of arrangements together with the specific destination countries would, when combined with other information reasonably available, create a realistic risk that individuals could be identified. This is of particular concern given the SFO's law enforcement function, where identifying staff and their locations could compromise their safety and security.

We also consider that disclosure would not constitute fair processing, since staff working overseas would have a reasonable expectation that this information would not be released in a way that could identify them.

Section 40(2) of the FOIA is an absolute exemption and we are therefore not required to consider the public interest in releasing the information requested.

Question 3

We confirm that we hold this information. However, this is exempt from release under section 31(1) of the FOIA.

Section 31(1)(a), (b), and (c) provides that:

Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice—

- (a) the prevention or detection of crime,*
- (b) the apprehension or prosecution of offenders,*
- (c) the administration of justice:*

How the exemption is engaged

As a law enforcement agency, the SFO holds highly sensitive information, which is of interest to others, including those we investigate. Disclosing detailed information about the specific security controls, configurations and capabilities applied to endpoint devices used by staff

working overseas could therefore compromise our ability to protect SFO investigative material and information systems, thereby prejudicing the interests at (a) (b) and (c) above.

Public interest test

Sections 31(a), (b), and (c) are qualified exemptions and require consideration of whether, in all the circumstances of the case, the public interest in exempting this data outweighs the public interest in disclosing it. More information about exemptions in general and the public interest test is available on the ICO's website at www.ico.org.uk.

It is recognised that there is a general public interest in publicising information about the SFO, so that the public knows that serious fraud, bribery, and corruption are being investigated and prosecuted effectively, and so that the public can be reassured about the general conduct of our organisation and how public money is spent.

However, having considered the public interest in releasing this information, we consider that the stronger interest lies in maintaining these exemptions of the FOIA. Primarily, the risk that this information could pose to the SFO's security systems against which it is essential to safeguard given the highly sensitive nature of the information held as a law enforcement agency. Releasing sensitive information about the specific technical security measures risk compromising the SFO's ability to provide and maintain data security for the cases at pre-investigation, investigation, prosecution stages and beyond.

Having considered the opposing arguments, I believe that the stronger public interest lies in exempting the information from release.