



Alicia Broadest

By email:  
[request-923773-2fd16899@whatdotheyknow.com](mailto:request-923773-2fd16899@whatdotheyknow.com)

**Freedom of Information Team**  
S1715  
6 Floor  
Central Mail Unit  
Newcastle Upon Tyne  
NE98 1ZZ

**Email** [foi.request@hmrc.gov.uk](mailto:foi.request@hmrc.gov.uk)

**Web** [www.gov.uk](http://www.gov.uk)

Date: 21 December 2022  
Our ref: FOI2022/74259

Dear Alicia Broadest,

**Freedom of Information Act 2000 (FOIA)**

Thank you for your request, which was received on 25 November, for information about our implementation of data encryption, cyber insurance policies and IT device losses that we have incurred. We have addressed your questions in turn, below.

- 1. “How many laptops, mobile, tablet or USB devices have been lost or stolen from your organisation in the past year (Sept 2021-Sept 2022)? Please specify numbers of each device type.”**

Loss (1 Sept 2021 – 31 Aug 2022):

BlackBerry or other mobile device	362
Microsoft Surface Pro tablet/Laptop Computer	123
USB Memory stick (encrypted)	2
USB memory stick (un-encrypted)	2

Theft (1 Sept 2021 – 31 Aug 2022):

BlackBerry or other mobile device	25
Microsoft Surface Pro tablet/Laptop Computer	121
USB Memory stick (encrypted)	0
USB memory stick (un-encrypted)	0

- 2. “How many of these devices were encrypted? Please specify numbers of each device type.”**

All HMRC standard issue devices are encrypted to HMG standards, and they are all deactivated remotely once they have been reported lost or stolen. These actions reduce the risk of unauthorised access to any data held.

With reference to the reported loss of 2 unencrypted USB memory sticks in the table above, occasionally some customers send data to HMRC on an unencrypted USB stick as untracked general post. If non-receipt is identified these are reported as security incidents and searches for the missing devices are undertaken in HMRC buildings and by the postal carrier. In such situations it is not always possible to establish if the device was ever received by HMRC as the loss may have already occurred before reaching us.

If you need extra support, for example if you have a disability, a mental health condition, or do not speak English/Welsh, go to [www.gov.uk](http://www.gov.uk) and search for ‘get help from HMRC’.

Text Relay service prefix number – 18001

**3. “Have you had to disclose or inform the ICO of a data breach as a result of any of these devices being lost or stolen in the past year (Sept 2021-Sept 2022)?”**

None of the incidents above required notification to the ICO. All HMRC standard issue devices are encrypted to HMG standards, and they are all deactivated remotely once they have been reported lost or stolen. These actions reduce the risk of unauthorised access to any data held.

**4. “Have you had to disclose or inform the ICO of a data breach for any other reason e.g., cloud breach, supply chain breach...”**

For information relating to data breaches notified to the ICO between September 2021 and March 2022, please refer to the latest [Annual Report and Accounts](#) (page 104).

All breaches notified to the ICO between April and September 2022 will be published in the 2022-23 Annual Report and Accounts. However, we can confirm there have been 12 ICO notifications to date in 2022-23.

**5. “How many data breaches (information has been lost, stolen, or taken from a system without the knowledge or authorisation of the department / organisation) have you experienced within your organisation (department) within the past year (Sept 2021-Sept 2022)?”**

Any personal data breaches involving ‘lost, stolen, or taken (data) from a system without the knowledge or authorisation of the department/organisation’ would constitute security incidents requiring formal notification to the ICO.

For information relating to data breaches notified to the ICO between September 2021 and March 2022, please refer to the HMRC’s [Annual Report and Accounts 2021-22](#).

Any breaches notified to the ICO between April and September 2022 will be collated and published in HMRC’s Annual Report and Accounts 2022-23. The publication date for this is yet to be confirmed.

**6. “Do you have an existing cyber insurance policy in place, and how long have you had it? If not, do you plan to invest in cyber insurance in the coming year?”**

No, we do not have an existing cyber insurance policy in place, nor do we plan to invest in cyber insurance in the coming year.

**7. “Have you had to claim on an existing cyber insurance policy in the past year (Sept 2021-Sept 2022) - if so, what was the reason for this i.e., ransomware attack, phishing scam...”**

Not applicable.

If you are not satisfied with our reply, you may request a review within 40 working days of receiving this letter by emailing [foi.review@hmrc.gov.uk](mailto:foi.review@hmrc.gov.uk) or by writing to our address at the top.

If you are not content with the outcome of an internal review you can [complain to the Information Commissioner’s Office](#).

Yours sincerely,

HM Revenue and Customs