Unencrypted Removable Media

Frequently Asked Questions

Q. What does encrypted and unencrypted mean?

A. Encrypted devices need a password/passcode for the user to access the information stored on the device whereas unencrypted devices do not.

The Department of Health has specified that personal confidential data can only be stored on a USB memory device if it has been encrypted to the appropriate NHS standard.

Q. What type of device does the removable media policy affect?

A. Any device that connects to your computer which can **store data** and is used for business purposes. This may include memory sticks (also known as data sticks, pen drives or flash drives), portable hard drives, dictation devices, memory cards and media card readers.

Items which do not store data such as USB fans, lights and speakers are not affected by this policy.

Q. How will the new removable media policy affect me?

A. The use of unencrypted removable media devices is being reviewed. Devices that are approved for business use will be added to the whitelist (a list of approved devices). Some items such as unencrypted USB devices will need to be replaced with an encrypted device and any device that isn't used for business purposes will be blocked.

Q. What is a whitelist?

A. The whitelist is a list of approved devices. Any devices which can store data that are not on the whitelist will be blocked.

Q. What if I have forgotten to tell you about a device? Will it just stop working?

A. If it is an unencrypted removable media device which stores data and we have not been informed and approved the device, it will most likely not be able to connect to the network.

If a device has been blocked, you will see a pop-up message at the bottom right of the screen that states “Access to device blocked by Sophos” the message will provide information on who to contact if you need to request that the device is considered for addition to the whitelist.

Q. Can unencrypted USB memory sticks be added to the whitelist?

A. No. All unencrypted memory sticks that have a valid business use must be replaced with an encrypted version that has been approved by NHIS.

Q. Which encrypted USB memory sticks can I buy and where can I buy one from?

A. The recommended devices are the Kingston Data Traveller Vault Privacy 3.0 or the Integral Courier FIPS 197 Encrypted USB.

Please note both Kingston and Integral provide several similar products and it is only these models above that are currently approved.

Integral Courier FIPS 197 Encrypted USB Part Codes

Capacity	Part Codes	EAN
8GB	INFD8GCOU3.0-197	EAN 5055288423978
16GB	INFD16GCOU3.0-197	EAN 5055288423985
32GB	INFD32GCOU3.0-197	EAN 5055288423992
64GB	INFD64GCOU3.0-197	EAN 5055288424005

Encrypted USB memory sticks can be ordered through your usual procurement channels or via the NHIS Business Relationships Team business.relationships@notts-his.nhs.uk or 01623 410310 and select option 3.

Q. Can things be added to the whitelist in the future?

A. Yes. An electronic form is being developed and will be available on the NHIS Customer Portal (https://customerportal.notts-his.nhs.uk/). All requests will need to be approved by your line manager, IG and NHIS.

Q. I already have an encrypted USB memory stick – will I still be able to use this?

A. The work being carried out is focusing on unencrypted removable media devices initially, therefore encrypted memory sticks will not be blocked at the current time.

Security standards are constantly improving across the world to protect against increasingly sophisticated cyber-attacks, therefore in the future we will need to ensure older encrypted devices still offer the required level of protection.

Q. Will I still be able to charge devices, e.g. my phone through the USB port after 31 July?

A. This will need to be tested. Blocking the 'data' element of the USB connection may prevent some phones from charging.

Q. When working from home I occasionally need to plug my own printer into my work laptop to print or scan documents – will I still be able to do this?

A. The removable media policy only affects devices which can store data so in most cases printers will not be blocked.