Removable Media Devices

Please contact your Information Governance lead for further information.
To order an encrypted USB memory stick please contact
business.relationships@notts-his.nhs.uk or 01623 410310 and select option 3.

Removable Media Devices

03
Removable media devices could also introduce viruses and malware to our IT network.
04
A list of approved devices and a new policy are being developed.
02
Only encrypted devices should be used when saving personal confidential or sensitive data and only used as a last resort.
05
Only removable media devices provided by your organisation should be used.
01
Removable media devices include external hard drives, USB memory sticks, media card readers and dictaphones.
06
Personal and unencrypted items should not be used and will be blocked in the coming months.

Please contact your Information Governance lead for further information.
To order an encrypted USB memory stick please contact
business.relationships@notts-his.nhs.uk or 01623 410310 and select option 3.

Removable Media Devices - FAQs

What does encrypted and unencrypted mean?

Encrypted devices need a password for the user to access the information stored on the device whereas unencrypted devices do not.
If you store sensitive data on a USB memory stick, the stick must be encrypted to protect the information from unauthorised access.

Which devices need to be added to the whitelist?

Please inform the IG team of 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 and IG **do not** need to be informed

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

The recommended devices are the Kingston Data Traveller Vault Privacy 3.0 or the Integral Courier FIPS 197 Encrypted USB.
To order an encrypted USB memory stick please contact the NHIS Business Relationships Team via business.relationships@notts-his.nhs.uk or 01623 410310 and select option 3.

Can things be added to the whitelist in the future?

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.

Removable Media Devices - FAQs

What does encrypted and unencrypted mean?

Encrypted devices need a password for the user to access the information stored on the device whereas unencrypted devices do not.
If you store sensitive data on a USB memory stick, the stick must be encrypted to protect the information from unauthorised access.

Which devices need to be added to the whitelist?

Please inform the IG team of 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 and IG **do not** need to be informed

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

The recommended devices are the Kingston Data Traveller Vault Privacy 3.0 or the Integral Courier FIPS 197 Encrypted USB.
To order an encrypted USB memory stick please contact the NHIS Business Relationships Team via business.relationships@notts-his.nhs.uk or 01623 410310 and select option 3.

Can things be added to the whitelist in the future?

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.