Protect, Don't Connect!

Unless it's a department-issued and approved device

Why can't I use my own USB key?

- For the official policy, see the Portable Storage Devices Directive.
- If you lose it, you've also lost the department's information on it.
- Department-issued USB keys are encrypted and comply with TBS security requirements to protect the information stored on them in the event the key is lost, misplaced, or stolen.
- Even if you buy a new USB key, it can't be used for work purposes. Store-bought USB keys have been known to be tampered with during production which makes them a risk. More importantly, work information can only be stored on department-issued equipment.

Have a business need for a USB key? → See Encrypted USB Devices

What about my cellphone, iPod, e-reader, smart watch, etc (anything personal that connects or charges via the USB port)?

- These are storage devices and by policy only approved and encrypted devices can be connected to the network.
- Even if you were not intending to use them to store work information, you still cannot plug them in. Your personal device could have a virus on it (even if you think it's clean) that could infect the network.

Bottom line: don't plug any personal devices into the USB ports.

This sticker should be on your computer in a visible location to remind you!

Questions? → See USB Storage Devices Q&A's

Need to charge your phone at work?

Use an electrical outlet to charge your phone or any other personal device.

Want more information?
Portable Storage Devices portal
Approved Portable Devices Do's and Don'ts
Easy Action Toolkit – USB Keys

Need help?
Email IT Security Centre of Expertise