

Data storage policy

Removable media

Introduction

This policy deals with the use of USB sticks and other removable media, such as CDs and DVDs, and is designed to set out clearly what is expected of OFT personnel to ensure sensitive and confidential information is handled correctly. This policy should be read in conjunction with Office Notice No. 01/08 - Revised rules for handling personal data which states that staff should 'not take any personal data outside OFT premises on unencrypted laptops or removable media like external hard drives, memory sticks, DVDs etc'.

All OFT staff have signed the Official Secrets Act and should be aware of their obligations. Further information is available in the Security Handbook.

Scope

What is 'removable media'? Although most of this document refers explicitly to USB sticks the policy covers any means of data storage that can be used for taking electronic information out of the OFT. This includes, but is not limited to, CD and DVD burning. Also, many consumer electronics gadgets such as PDAs, Blackberries, iPods and even phones can be used for removable data storage.

What are memory sticks?

USB sticks are small yet capacious. Their size makes them convenient to carry but also makes them easy to have stolen or to lose. A memory stick can contain thousands of documents and large databases. Whole directories can be put onto a stick without checking exactly which files are being copied and what their individual security classification is. It is also possible that if the stick is taken away and used on a virus infected PC, many corrupted documents may then be put back onto the OFT

network. At the very least you could lose a vital document. It's also worth remembering that these sticks can, on occasion, fail and information may be lost. USB sticks must only be used for the temporary transfer of documents.

How do I get a memory stick?

- IT Group will keep a stock of memory sticks which, subject to a satisfactory business case, we will issue to applicants who have supplied a request endorsed by a line manager of at least Grade 7 level, accompanied by a business case.
- IT Group will make sure that any request for a memory stick is supported by a business case covering the following key points:
 - What sort of information is to be put on the stick?
 - Could any information stored on the stick be considered as 'personal data'?
 - Does the information have a security classification or is it market sensitive?
 - What is to be done with the data when it's on the stick (e.g. will it be take it home and used on a non-OFT machine)?
 - What steps will be taken to erase data that is no longer need on the stick?

Rules about memory stick use

- Ensure that portable storage devices are not being used to store sensitive, confidential or personally identifiable information without prior consultation with IT Group.
- Do not use the memory stick to store 'personal data'. For the definition of personal data and for further advice on the rules pertaining to such information please see Office Notice No. 01/08.
- Staff must obtain approval from their line manager (who must be at least at Grade 7 level) before creating, moving or copying information, files, folders etc onto a portable storage device.
- Ensure that portable devices are stored securely when left unattended. Devices taken off-site should not be left unattended in public places or at individual's home address.
- Ensure that information held on portable storage devices is not automatically copied (backed-up). To avoid total loss of data, users

must ensure that information stored on portable storage devices is 'backed-up' and held in the appropriate place on the OFT Network.

- If a portable storage device is lost, stolen or mislaid it must be reported immediately to the your line manager and the IT Helpdesk.
- You must only use equipment that has been purchased or approved by the Office of Fair Trading's IT Group. The use of personal equipment is not allowed on our IT infrastructure.
- Staff are responsible for ensuring that visitors or contractors who bring their own USB devices into the OFT (to give a presentation for example) are supervised at all times whilst the device is connected to OFT equipment.
- OFT PCs automatically scan USB memory sticks. However staff are responsible for scanning when off site. The device should be used carefully and use in untrusted PCs should be avoided.

Summary

In short, if you need to take any information from the OFT network out of the OFT consider whether the information would be damaging to the OFT if it was lost. If so please contact the IT Help Desk for advice on the safest way to proceed.