

|  |  |
| --- | --- |
| < Insert name of pharmacy>**Mobile computing and Bring Your Own Device** | <Insert pharmacy logo> |
| Doc prepared by: | Doc approved by: | Date next review due: |  |  |
| Date prepared: | Date approved: | Date review takes place: |  |  |

|  |
| --- |
| ***About the use of this document and related resources****: This* [*data security*](http://psnc.org.uk/ds) *document assists the pharmacy’s aligment with the*[*Data Security and Protection Toolkit (DSPTK)*](http://psnc.org.uk/dsptk)*. Related pharmacy policies are at PSNC’s* [*data security templates webpage*](http://psnc.org.uk/dstemplates)*.* |

**Tip: If the pharmacy does not use any mobile computing**: i.e. there are no laptops and PDAs, nor any portable device used to hold or transfer personal information (e.g. USB sticks and CDs/DVDs), the pharmacy can indicate within the Data and Security and Protection Toolkit (DSPTK) for any relevant questions, that this is the policy.

This document outlines the guidelines that should be followed by staff when using portable computer devices, mobile phones and removable media.

**Definitions:**

**Portable computer devices**: this includes laptops, notebooks, tablet computers, PDAs (personal digital assistants) and mobile phones.

**Removable data storage media**: this includes any physical item that can be used to store and/ or move information and requires another device to access it. For example, CD, DVD, floppy disc, tape, or digital storage devices (flash memory cards, USB disc keys, and portable hard drives). Essentially anything you can copy, save and/or write data to which can then be taken away and restored on another computer.

**Bring Your Own Devices (BYOD) policies**: BYOB policies may be set out by the IG Lead and the leadership of the organisation and such policies may be in place to make clear where staff home devices can be used for work purposes where there is no transfer of sensitive information e.g. to check work-related websites. Some pharmacy contractors will set out a BYOB policy which does not allow use of personal devices during working time.

**Scope**

This guidance applies to all pharmacy staff including temporary staff.

Only authorised staff should have access to portable computer devices and digital storage devices such as flash cards, USB disc keys and portable hard drives. Any member of staff allowing access to any unauthorised person deliberately or inadvertently may be subject to disciplinary action.

Staff should not use unauthorised portable devices or digital storage device (such as personal phones) for storing or communicating sensitive information.

**Use of portable computer devices**

***DO …***

Store portable equipment securely when not in use on site

* Store portable equipment securely when not in use off site
* Set up access controls, for example a personal password, where possible
* Ensure files containing personal or confidential data are adequately protected e.g. encrypted
* Ensure that PDAs are configured so that they lock after a maximum period of 5 minutes inactivity. Once locked the PDA should be set to require password authentication to resume use.
* Install password protected screensavers on laptops
* Use and regularly update anti-virus software
* Take regular backups of the data stored on the portable equipment
* Obtain authorisation prior to the removal of portable equipment from the premises
* Be aware that software and any data files created by staff on Pharmacy portable computer devices are the property of the Pharmacy
* Report immediately any stolen portable equipment to the police and line manager
* Be aware that the security of your portable computer device is your responsibility and you should check your home and car insurance policies to ensure they cover for business use
* Ensure that portable devices are returned to the pharmacy if you are leaving employment

***DO NOT …***

* Use your own portable computer device or digital storage device such as flash cards, USB sticks and portable hard drives) for pharmacy business unless authorised
* Leave portable equipment in places where vulnerable to theft
* Leave portable equipment visible in the car when travelling between locations
* Leave portable equipment in an unattended car
* Leave portable equipment unattended in a public place
* Install unauthorised software or download software / data from the internet
* Disable the virus protection software
* Use portable computer devices outside the pharmacy premises without authorisation
* Allow unauthorised personnel/friends/relatives to use portable equipment in your charge
* Delay in reporting lost or stolen equipment,
* Attach unauthorised equipment to the network
* Remove personal information off site without authorisation

**Bring Your Own Device (BYOD) guidelines**

See: [DSPTK series template\_08B\_ Bring Your Own Device \_guidelines and policy](https://psnc.org.uk/dstemplates)

Bring Your Own Device (BYOD) is the practice of allowing staff to utilise personally owned devices (such as smartphones, tablets or laptops) in the workplace, and to use those devices to securely access the organisation’s systems, applications and information. BYOD is optional and offered to provide greater flexibility. It may not be available to all staff.

|  |
| --- |
| *This data security policy assist the pharmacy’s aligment with the Data Security and Protection Toolkit (DSPTK). Related pharmacy policies and more can be found at:** [*psnc.org.uk/ds*](http://psnc.org.uk/ds)*;*
* [*psnc.org.uk/dsptk*](http://psnc.org.uk/dsptk)*; and*
* [*psnc.org.uk/dstemplates*](https://psnc.org.uk/dstemplates)*.*

*Pharmacy contractors with queries about the original template or questions about DSPTK may contact* *it@psnc.org.uk**.*  |