

|  |  |
| --- | --- |
| < Insert name of pharmacy>**Bring your own devices policy and guidelines** | <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)*.* |

*Note: This document is intended to be used in conjunction with:*[*DS&IG 08A Portable computer devices guidelines*](https://psnc.org.uk/dstemplates)*.*

**Introduction**

Bring Your Own Device (BYOD) is the practice of allowing staff to utilise personally owned devices (such as smartphones, computers tablets or laptops) for work, 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 policy provides guidance which must be followed when using your own device at work. All users of BYOD are required to read this policy in full and confirm they understand and will comply with it. A summary of important points is provided below.

|  |  |
| --- | --- |
| **Do** | **Don’t** |
| Keep your passwords secure | Don’t share your device or passwords  |
| Use biometric features to secure the device if possible | Don’t make copies of data or take screenshots  |
| Keep your operating system updated | Don’t access systems without authorisation |
| Be careful who can see your screen when accessing work systems | Don’t save work in unapproved locations or applications |
| Consider using ‘Find my device’ and global positioning system (GPS) features if these are available on the device to help in the event of device loss |  |
| Report lost or stolen devices |  |
| Be aware of your responsibility for all costs  |  |
| Facilitate IT to conduct spot checks if required |  |
| Inform IT if you leave employment with the organisation |  |

**Scope**

This policy applies to all staff and authorised third parties of the organisation who voluntarily choose to use BYOD.

The BYOD service includes a range of systems and access may vary by individual depending on the requirements of individual roles.

Available systems include:

* email;
* calendar;
* intranet and web browsing;
* internal web-based systems;
* rotas and scheduling;
* communication systems;
* reporting systems; and
* clinical systems.

**Aims**

* To ensure BYOD systems and data are used appropriately, legally and securely.
* To ensure personally owned devices are used in a manner which protects confidentiality in accordance with GDPR.
* To ensure staff clearly understand their responsibilities when using BYOD.

**Support Devices**

Due to the rapid pace of change it is not possible to support BYOD on all devices.

BYOD may only be supported on devices which will run the latest version of the Apple or Android operating system. Staff will be expected to ensure devices are kept updated or risk losing access to some systems.

Devices must be encrypted and have passcode or biometric security if available with a timeout to lock automatically after 5 minutes of inactivity. Jailbroken or rooted devices are strictly prohibited. Staff must not circumvent security controls.

The organisation’s BYOD software may be installed on devices for access to be granted to systems. Staff should not remove or modify the BYOD software on their device.

Technical support will be limited to the organisation’s BYOD software and systems.

Connectivity via WiFi or mobile data contracts will be the responsibility of the device owner. Digital information must only be downloaded or uploaded over a secure connection. It must not be downloaded over a public WiFi network because of the lesser security within public WiFi networks e.g. avoid downloading sensitive information using public WiFi from airports, hotels, coffee shops, public transport etc.

**Access**

Use of BYOD and access to corporate systems is subject to other organisation policies and practices and does not override or supersede them.

BYOD is optional and may not be appropriate in all roles.

The organisation reserves the right to revoke access if staff do not follow this policy.

**Responsibilities**

Staff may only connect to organisation systems for the purpose of authorised work.

Use of a device that has access to work systems via BYOD should be limited to its owner and must not be shared. Devices must be maintained as stated in section 4.

Account logon, passwords and pins must be kept confidential and never shared with others.

Staff should be conscious of the setting in which devices are being operated and should ensure data and systems displayed are not visible to others. Data accessed must not be saved to the device or copied off it. Screenshots of systems must not be taken.

Staff must inform senior staff if they leave employment with the organisation.

Staff must comply with all relevant legislation including not using BYOD whilst driving.

Staff must read and understand and adhere to other key policies such as data security policies.

Staff must immediately inform the relevant person(s) if:

* their password has been breached;
* Their device gets lost or stolen; or
* organisational systems are not working normally.

**Loss or Damage**

* The organisation will not accept any liability for loss or damage of personal devices and data that are using the BYOD system.
* Staff should inform the relevant person(s) immediately if they lose their personal device or have it stolen.
* There may be ways to block the device being able to access work areas.

**Acceptable Use**

* Staff should typically only use the BYOD policy to access work systems during working hours.
* Staff should only access systems which they require and normally use.
* Staff should never try to access systems for which they are not authorised.
* Confidential data should only be accessed for a specific work-related requirement.
* Any suspected breach must be immediately reported to IT.

**Costs**

Staff are solely responsible for all costs associated with purchasing, running, repairing and replacing their personal devices used with BYOD.

Staff are responsible for all mobile data or WiFi hotspot costs related to BYOD usage and should monitor these to ensure they have sufficient allowance.

**Monitoring**

Staff may be asked not to use their device for certain/all purposes if it is identified that the device is not suitably secure e.g. running on an older operating system.

Some systems such as the NHSmail app should auto detect if the device or operating system is too old to enable it to run – see below.

**NHSmail**

NHSmail may be used on personal or work mobile devices. NHS Digital have an arrangement with Microsoft for the provision of NHSmail and therefore NHSmail is compatible with Microsoft’s Outlook apps.

The Outlook mobile app is available from the Apple/Android app store for download/update onto Apple/Android mobile devices e.g. iPhones or Samsung mobile phones. .

The NHSmail app should auto-detect if the device or operating system is too old to enable it to run. However, it is recommended that Outlook mobile app users update the app to receive the most up-to-date versions and features. The most recent versions of the Outlook app might fail to work with some aged mobile devices efficiently, or at all.

Staff using personal devices should schedule the ‘Do Not Disturb’ setting, to prevent receipt of work-related messages outside of work hours. This is important to reduce the risk that those who are working do not believe that the NHSmail will be dealt with. It is also important to support the need for staff to ensure they maintain a healthy work/life balance.

The NHSmail ‘Do Not Disturb’ mode can be scheduled to occur for set hours each day/week and can also be easily toggled off and on. Personal mobile devices may also have a broader ‘Do Not Disturb’ mode for preventing notifications of any kind – such as when periods of concentration/non-notification are required.

Personal shared mailboxes can be accessed via the Outlook mobile app. This NHSmail feature had been requested by pharmacy NHSmail users and others, so that pharmacy contractors / teams using a pharmacy BYOD policy could choose to be able to be auto-notified if an email arrives at the NHSmail shared box.

Pharmacy NHSmail users and pharmacy contractors that wish to use NHSmail on mobile devices will also have to be aware of various practical considerations, such as:

* Passcode/biometrics settings.
* Preventing access by others.
* Considering adjusting auto-preview of messages on home-screens if required.
* Having the ability to remotely wipe the device if stolen.
* Storage and archive settings.
* Processes if a member of staff will leave the pharmacy (the account may be removed from the personal Outlook app and the staff member or pharmacy team may unlink the personal account from the shared pharmacy mailbox once this becomes required).Pharmacy-facing guidance may be available at the PSNC website about pharmacy use of NHSmail – including use of NHSmail with mobile devices - [psnc.org.uk/nhsmail](https://psnc.org.uk/nhsmail).

**Notes about this policy**

This template is based on a version prepared by NHSX for use within health and care. The template above may be adapted by pharmacy contractors.

|  |
| --- |
| *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**.*  |