North West London
Collaboration of
Clinical Commissioning Groups

NWLCCGs Bring Your Own Device (BYOD) Policy

V1.3 September 2020

Version Control

Version Number	Reviewing Committee / Officer	Date
1.0	NHS NWL Clinical Commissioning Group, IT Security & Cyber Security Team	January 2019
1.1	Bill Sturman	15 Jan 2019
1.2	Abhilash Abraham	15 Jan 2019
1.3	Data Protection Officer (Corporate) Data Protection Officer (GP)	29 June 2020

Reviewers

This document must be reviewed by the following:

Name	Signature	Title / Responsibility	Date	Version
Bill Sturman		Director of Informatics/SIRO NW London CCGs	15/1/19	1.0
Abhilash Abraham		IT Security & Cyber Security Lead	11/3/19	1.2
Felicia Ayo-Ajala Dr. Ernest Norman-Williams		Data Protection Officer (Corporate) Data Protection Officer (GP)	29/06/20 29/06/20	1.3 1.3

Approvals

This document must be approved by the following:

Title	Signature	Title / Responsibility	Date	Version
Bill Sturman		Director of Informatics/SIRO NW London CCGs	12/03/19	1.2
Victoria Medhurst		Head of Governance/SIRO	28/08/20	1.3
NWL CCGs Governing Bodies	------	NWL CCGs Governing Bodies	Sept 2020	1.3

Contents

Introduction

This Policy applies to North West London Collaboration of Clinical Commissioning Groups (NWL CCGs), subsequently referred to in this document as NWL CCGs. only and not to their associated GP Practices

The underlying feature of Bring Your Own Device (BYOD) is that the user owns, maintains and supports the device. This means that the data controller for any organisational data accessed on the device (the employing organisation) will have significantly less control over the device than it would have over a traditional corporately owned and provided device.

Whilst ownership is not corporate, responsibility for the ownership of the data remains with the data controller. It is important to remember that the data controller must remain in control of the personal data for which they are responsible, regardless of the ownership of the device used to carry out the processing.

Connection of a personally owned device to corporate networks is subject to all organisational policy in respect of information security and the protection of data and equipment.

Purpose

Bring Your Own device (BYOD) can be seen as a means of obtaining cost and resource efficiencies as the staff member may be providing the equipment e.g. Smartphone, Laptop etc. rather than the organisation purchasing this directly for them.

The Bring Your Own Device Policy shall be used to enable appropriate controls and procedures to be enforced on personal devices that have been authorised to process NHS data.

Scope

This policy applies to all employees (permanent, seconded, contractors, management and clinical trainees, apprentices, temporary staff and volunteers) of NWL CCGs.

Third Parties with whom the NWL CCGs may agree information sharing protocols will be governed by this policy and associated information sharing agreements. The term Third parties in this context refers to any employees who are not directly employed by NWL CCCGs but have access to NWL CCGs resources as part of their role e.g. contractors, temporary staff.

NWL CCCG's Current BYOD Status

Mobile working solutions and VPN (Virtual Private Network – remote connection) connections are only permitted on corporately owned devices, because of the significant support requirements, device management and encryption, in addition to end user training requirements.

NWL CCGs current policy is not to enable any connections to our network from personally owned device until a secured MDM solution is procured and deployed for such technologies. Subject to funding, such a solution is expected in 2019/2010. After that, any user seeking to connect a personally owned device to NWL CCGs network via a named account (rather than as a guest), must gain authority via their line management structures to connect and if applicable provide a budget code to meet the cost of the connection of the device to an Mobile Device Management (MDM) Solution. A 'BYOD access request form' must be submitted to the IT Service Desk.

BYOD and NHSmail

NHSmail is the email system for transfer of personal confidential data (PCD) as the system is encrypted end-to-end. As a user of the NHSmail platform, individuals must operate in accordance to a clear set of guidance, policies and procedures to ensure the service is being used effectively, appropriately and safely. Every NHSmail user is required to accept the Acceptable Use Policy when they register for the service.

While using the NHSmail Web function staff must also abide by the following rules:

a) Ensuring that if NHSmail is being accessed via the Web, staff must not auto save the password on their device;

b) If accessing NHSmail Web on a personal device (such as an iPhone) staff must ensure that a screen saver prompting a mandatory password is kept on the device at all times.

c) Staff must be vigilant of the environment in which they access e-mails and ensure confidentiality is maintained at all times (e.g. if accessing from a home computer ensure that no friends or family members are able to see e-mails);

d) Always check that NHSmail is logged out after use.

As the personal device used to access NHSmail Web will likely not be encrypted staff must not save any emails outside the secure web portal.

Should an individual wish to use either a personal device to connect to NHSmail, or a mobile device that cannot be encrypted or allow the NHSmail organisational policies to be applied, they must have approval from their own organisation to ensure compliance with local information governance policies.

Duties and Responsibilities

NWL CCGs have a legal duty to comply with the GDPR 2016 and the Data Protection Act 2018. The Accountable Officer is responsible for ensuring that the responsibility for data protection is allocated appropriately within NWL CCGs and that the role is supported.

All staff must adhere to NWL CCGs policies and procedures relating to the processing of personal information, and the data controller (organisation) must assure themselves that the technical solutions for the security of data are sufficient for the data being processed, specifically where these risks are increased through mobile working and personal ownership of devices.

All devices shall be configured and operated in accordance with this policy and the organisation shall determine which types of devices are relevant to this policy.

Organisational Policy

This policy should be read in conjunction with other relevant organisational Policies i.e. Information Security Management System (ISMS).

NWL CCGs grant their employees the privilege of purchasing and using smartphones and tablets of their choosing at work for their convenience. The organisation reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined above.

This policy is intended to protect the security and integrity of the NWL CCGs data and guard against both data leakage and data loss.

Acceptable Use

Employees remain subject to organisational policy and procedure in respect of personal conduct, data and information security, and physical security, including but not limited to those policies outlined above.

Devices may not be used at any time to:

- Store or transmit illicit material

- Store or transmit proprietary information belonging to another organisation
- Harass others
- Engage in outside business activities

NWL CCGs has a zero-tolerance policy for texting or mailing while driving and only hands- free talking while driving is permitted – provided that it is safe and legal to do so.

Devices and Support

NWL Service Desk will discuss the connection of any device with the end user, to ensure that the device is authorised and can be connected.

In regard to support, personal owned devices are not organisationally supported devices. Only connectivity issues are supported, employees should contact the device manufacturer or their carrier for operating system for hardware-related issues.

Reimbursement

NWL CCGs will not reimburse the employee for the cost of purchase or associated with the device including but not limited to:

Roaming charges, plan charges and overcharges and applications for personal use.

Security

Employees' access to the organisation's data is limited based on user profiles defined by organisational policy and is automatically enforced. An essential element of maintaining the security of the data is that the BYOD applications are managed and controlled.

In order to ensure that maximum protection is provided against malicious code, the permitted devices shall:

- Permit security patches and updates to be installed
- Be devices that shall enable the use of Mobile Device Management (MDM).

Users shall be required to update devices as soon as the update becomes available.

For note for each organisation user and authoriser are associated risks of NWL Service Desk Opening hours, excluding public holidays. Devices lost, stolen or otherwise compromised during times when the service desk is closed are to be reported as soon as possible following the event.

Any attempt to side step or circumvent security measures in place will be considered under the NWL CCG disciplinary policies, this includes any attempt to 'screen capture' or otherwise photograph content to enable its onwards transmission outside of security parameters.

All users are required to report any incident on their BYOD as they would for any NWL CCG IT equipment.

Risks/Liabilities/Disclaimers

The organisation reserves the right to disconnect devices or disable services without notification should a security incident or risk occurs. NWL CCGs reserves the right to take appropriate disciplinary action.

Lost or stolen devices must be reported to the NWL Service Desk as soon as possible. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.

The employee is expected to use his or her devices in an ethical manner at all times and adhere to the NWL CCGs related acceptable use policies.

The employee is personally liable for all costs associated with his or her device

References

Information Commissioners Office Bring Your Own Device: https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf

NHS Digital:

https://digital.nhs.uk/services/data-and-cyber-security-protecting-information-and-data-in-health-and-care/cyber-and-data-security-policy-and-good-practice-in-health-and-care/bring-your-own-device-byod-guidance-for-health-and-care-organisations

NHS
North West London
Collaboration of
Clinical Commissioning Groups

Appendix 1

Equality Impact Assessment Tool (Equality Analysis)

To be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval.

		Yes/ No	Comments
1	**Does the policy/guidance disadvantage one group or more than another on the basis of:**		
	• Race (including colour, culture, ethnicity, nationality or national origin and the travelling community)	N	
	• Religion or Belief	N	
	• Sex (e.g. male or female)	N	
	• Marriage or Civil Partnership	N	
	• Sexual Orientation (Lesbian, Gay, Bisexual, Heterosexual)	N	
	• Gender reassignment (e.g. someone who 'is proposing to undergo, is undergoing or has undergone a process (or part of a process) for the purpose of reassigning the person's sex by changing physiological or other attributes of sex.')	N	
	• Disability (e.g. learning disabilities, physical disability, sensory impairment, mental health problems etc.)	N	
	• Pregnancy and Maternity	N	
	• Age (children, young adolescent, older people etc.)	N	
2	**Is the policy/guidance/strategy more favourably towards one group on the basis of:**		
	• Race	N	
	• Religion or Belief	N	

	• Sex	N	
	• Marriage or Civil Partnership	N	
	• Sexual Orientation	N	
	• Gender reassignment	N	
	• Disability (e.g. learning disabilities, physical disability, sensory impairment, mental health problems etc.)	N	
	• Pregnancy and Maternity	N	
	• Age (e.g. children, young adolescent, older people etc.)	N	
3	**If you have identified potential discrimination in the policy/guidance are there any valid, legal and/or justifiable exceptions? Please list any exceptions.**	N/A	
4	**Is the policy/guidance likely to have a negative/adverse impact on any of the above group(s)?**	N/A	
5	**If so, how would you address the impact? Please explain.**	N/A	
6	**What are the associated objectives to the policy/guidance?**		See section 2 of policy

If you have identified a potential discriminatory impact in this document, please refer to the author(s) of the policy/guidance, together with any suggestions required to address the impact.