Ref: (IG 15)

BRING YOUR OWN DEVICE POLICY

Executive Sponsor & Function	Chief Digital Officer
Document Author:	Cyber Security Manager
Approved by:	Quality, Safety and Performance Committee
Approval Date:	12th March 2026
Date of Equality Impact Assessment:	9th February 2026
Equality Impact Assessment Outcome:	Approved
Review Date:	9th February 2027
Version:	1

TABLE OF CONTENTS

1. AIM

This Policy is one of a set of policies, which sit beneath the All-Wales Information Security Policy, and assists the Velindre University NHS Trust ("VUNHST") to maintain compliance with its statutory responsibilities and duties.

VUNHST does not require, expect, or encourage staff to use their personal devices to access work emails, Microsoft Teams messages, or any other work-related systems outside of their normal working hours. While BYOD access is available for convenience, it is entirely optional. Staff are reminded of the importance of maintaining a healthy work–life balance and should feel confident in disconnecting from work-related digital services when off duty.

Whilst it is recognised that use of personally owned devices for work purposes brings many benefits, such devices also pose a high security risk if they are left vulnerable to theft, loss and unauthorised access.

This BYOD Policy sets out clearly how VUNHST exercises its responsibilities for the confidentiality, integrity and availability of VUNHST information and personal data and the acceptable use of personal devices by staff to access VUNHST data, which may include data about staff, patients, donors, suppliers and other business connections.

VUNHST provides external access to various VUNHST services for all of its staff, as well as other authorised users, for purposes that are of benefit to both VUNHST and to the user in the work they undertake on behalf of VUNHST. However, ultimately it is up to the staff member to decide whether they wish to make use of this facility, and if they choose to do so they must ensure that they maintain a healthy work-life balance whilst doing so.

The services currently accessible by BYOD are subject to change but include (*See Bring Your Own Device Accessible Applications in Appendix 1*):

- Microsoft 365 applications including, but not limited to:
  - Microsoft Teams
  - Outlook (e-mails & calendar)
  - OneDrive
  - SharePoint
  - Office apps (Word, Excel, PowerPoint)
- ESR

VUNHST will monitor access to these resources but will not monitor the content or usage of a personal device under any circumstances.

2. POLICY STATEMENT AND OBJECTIVES

The objective of this policy is to:

- protect the confidentiality, integrity and availability of VUNHST data.
- ensure that BYOD users are aware of their responsibilities when accessing VUNHST data on personal devices.
- provide guidance and set expectations for what can and cannot be achieved with the BYOD system in place.
- ensure that BYOD users are aware of the consequences of breaching this policy.

3. SCOPE OF THIS POLICY

This policy applies to anyone who accesses or processes VUNHST data on personally owned devices.

4. ROLES AND RESPONSIBILITIES

Chief Executive Officer

The Chief Executive Officer ("CEO") has overall responsibility for Data Protection and Confidentiality within VUNHST. As accountable officer, they are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support the safe and secure handling of information.

To satisfy the above, the CEO has delegated this responsibility to the Executive Director of Finance. The Executive Director of Finance is accountable for the Trusts overall Information Governance arrangements.

Caldicott Guardian (CG)

The Executive Medical Director has been nominated as the Trusts Caldicott Guardian and has specific responsibilities regarding confidentiality and consent, in relation to personal data.

Senior Information Risk Owner (SIRO)

The Executive Director of Finance is also the identified Senior Information Risk Owner (SIRO) and will take ownership of information risk. The SIRO is a key factor in successfully raising the profile of information risks and embedding information risk management into the Trusts culture.

Data Protection Officer (DPO)

The Head of Information Governance is appointed as the Trust's Data Protection Officer and has delegated responsibilities from the Chief Executive specifically regarding compliance with Data Protection legislation and the rights of data subjects. The Information Governance structure sits under this role.

Chief Digital Officer

The Chief Digital Officer has overall responsibility for the technical infrastructure to ensure the security and data quality of information assets and systems held within the Trust.

Information Governance

The Information Governance department are jointly responsible with Digital Services for the implementation, monitoring and review of this policy, as well as ensuring advice and guidance on technical specifications is made available to all staff.

They are also responsible for supporting managers when investigating breaches of this policy.

Digital Services

Digital Services, including Cyber Security, are jointly responsible with the Information Governance department for the implementation, monitoring and review of this policy, as well as ensuring advice and guidance on technical specifications is made available to all staff.

Managers

All Managers are directly responsible, ensuring that:

- users are aware of this policy.
- users are made aware of changes to this policy.
- users are trained appropriately.
- suspected incidents are reported and investigated.
- work in collaboration with the Digital Services department to ensure appropriate plans, business cases etc. are in place to support the procurement, maintenance/support and renewal of critical operational and clinical IT systems.

Users

Users are responsible for their own actions and must:

- adhere to this policy and associated policies and procedures.
- report incidents to appropriate managers as quickly as possible.
- report to Digital Services if a personal device is lost or stolen and log the incident on Datix.
- ensure ongoing awareness of this policy.
- ensure that they are up to date with their mandatory Information Governance training.

5. POLICY

Access Control

Users **MUST** only access VUNHST services and data from devices that they personally own. i.e. Users **MUST NOT** use shared devices such as those found in public places e.g. libraries.

Access to services and data is provided over a secure connection, generally via HTTPS.

Multi-factor authentication (MFA) is mandatory for accessing M365 services.

Users must not share their login credentials with anyone.

Data Security

Users must ensure that their personal device is secure and has appropriate security measures in place, such as PINs, passwords, biometric locks, up-to-date security software, and is updated with the latest operating system and software security updates.

Sensitive data must not be stored locally on personal devices.

Users must report any lost or stolen devices immediately to Digital Services.

Confidentiality

Users must maintain the confidentiality of all data when accessed from personal devices.

Monitoring and Compliance

VUNST and NHS Wales reserves the right to monitor access and usage of M365 services.

Regular audits will be conducted to ensure compliance with this policy.

Users must comply with all Trust policies regarding the use of personal devices, including but not limited to policies on data protection, patient confidentiality, and acceptable use.

Non-compliance may result in disciplinary action, including termination of employment.

Acceptable Use
Personal devices must not be used to access, store, or transmit patient, donor or organisational data unless authorised.

Users must comply with the organisation's data protection and confidentiality policies.

Any form of illegal activity or violation of organisational policies using personal devices is prohibited.

6. EQUALITY IMPACT ASSESSMENT STATEMENT

An EQIA has been completed, and its summary is presented at the front of this Policy.

7. GETTING HELP

Staff that require assistance should contact the Cyber Security Team in the first instance.

8. RELATED POLICIES

- Information Governance Policies.
- Information Security & Supplier Management Policies.
- Data Protection Impact Assessment Procedure.
- Incident Response Plan.
- Information Governance Policy.
- Data Quality Policy.
- Information Security Policy.
- Internet Use Policy.

- Email and Instant Messaging (EIM) Use Policy.
- Safeguarding and Public Protection Policy

9. INFORMATION, INSTRUCTION AND TRAINING

Staff are required to undertake the Information Governance and Cyber Security training every two years as part of the statutory/mandatory training.

APPENDIX 1

BRING YOUR OWN DEVICE ACCESSIBLE APPLICATIONS

1. ESR (Electronic Staff Record)
2. Microsoft Outlook
3. Microsoft Teams
4. Microsoft OneDrive
5. Microsoft SharePoint
6. Microsoft Authenticator
7. Microsoft Edge
8. Microsoft Company Portal
9. Microsoft Office
    a. Excel
    b. Word
    c. PowerPoint
10. Microsoft 365 Copilot
11. Microsoft OneNote
12. Microsoft To Do: Lists & Tasks
13. Microsoft SharePoint
14. Microsoft Planner
15. Microsoft Whiteboard
16. Power Platform
    a. Power Apps
    b. Power Automate
    c. Power BI
    d. Power Pages
    e. Copilot Studio
    f. Dataverse
    g. AI Builder