Ymddiriedolaeth GIG Prifysgol Felindre
Velindre University NHS Trust

Ref: IG 05

SOFTWARE POLICY

Executive Sponsor & Function	Executive Director of Strategic Transformation, Planning and Digital / Deputy CEO
Document Author:	Assistant Director of Digital Delivery
Approved by:	Quality, Safety and Performance Committee
Approval Date:	13 January 2026
Date of Equality Impact Assessment:	November 2025
Equality Impact Assessment Outcome:	No impact
Review Date:	January 2029
Version:	5

1. INTRODUCTION

1.1 Software refers to the collection of programs, applications, and digital services that enable computing devices, including desktops, laptops, servers, tablets, and mobile phones to perform specific tasks. It encompasses both traditional system software and modern mobile applications, distinguishing itself from hardware, which comprises the physical components of a device.

1.2 It is illegal to make or use unauthorised copies of software. As a result, legal action may be taken against both the organization and Trust employee (penalties for so doing include imprisonment and/or fines). It is the responsibility of staff not to make illegal copies and the responsibility of managers to ensure that this is practice does not occur.

1.3 The installation of unauthorised software poses a significant risk to the integrity and performance of Trust IT systems and increases the likelihood of information security breaches. This risk applies to software from all sources, including public domain applications, internet downloads, and content bundled with magazines or other media.

To mitigate this risk, only software explicitly authorised by the local Digital Services team may be installed on Trust-managed devices, including desktop PCs, laptops, servers, tablets, and mobile phones.

1.4 The Trust must ensure that all staff are aware of the policy and comply with it. Therefore, the scope is:

- All Trust use of Software
- All Trust staff (outside personnel under Trust staff guidance are the responsibility of that staff member e.g., students, volunteers & visiting colleagues)
- All staff of Velindre hosted organisations
- All Trust Honorary Contract holders
- Third party contractors i.e. medical device manufacturers / support – Note: need to identify how this will be communicated out of the policy i.e. contract terms & conditions

2. STATEMENT REGARDING THE USE OF COMPUTER SOFTWARE

2.1 Velindre University NHS Trust licenses the use of computer software from a variety of external companies and other non-commercial sources. The Trust does not have the right to alter, copy or distribute software unless authorised by the software developer or vendor under the license agreement. Software licensed by the Trust must not exceed license allocation; therefore, software cannot be installed onto additional corporate or home computers without the consent / involvement from the local Digital Services department.

2.2 Software license agreements may apply to single machine use, multiple machines, single or multiple users, or use on Local Areas Networks (LANs). In all circumstances, Trust employees are required to comply with license agreements.

Advice on appropriate licensing arrangements for software should be sought from the Digital Services department.

2.3 Trust employees learning of any misuse of software or related documentation within the Trust must notify the department manager or the local Digital Service Desk.

2.4 According to UK Copyright Law, illegal reproduction of software can be subject to civil damages with no financial limit, and criminal penalties, including fines and imprisonment.

2.5 Installation of unauthorised software and / or personal content (including, but not limited to documents, pictures, audio & video files etc.) on any Trust computers can affect the proper operation of those computers and increase the risk of information security breaches or introduce clinical risk and is therefore not permitted.

2.6 Trust employees who make, acquire or use unauthorised copies of computer software or install personal content will be subject to the formal disciplinary process. This may include termination of employment. The Trust does not condone the illegal duplication or use of software.

3. OBJECTIVES

- To ensure that Velindre University NHS Trust complies with the law
- To protect our corporate reputation
- To comply with the information security policy
- To protect our investment in IT
- To increase control of software resources
- To increase discipline among staff who under-estimate the value of software
- To ensure corporate machines operate effectively
- To reduce the financial risk through potential litigation
- To ensure the use of software within Velindre University NHS Trust aligns with national (NHS Wales / Welsh Government) policies and standards, such as the requirement to deliver digital services 'cloud first'.

4. ROLES AND RESPONSIBILITIES

4.1 Organisation

Organisation responsibilities are:

- To provide appropriate solution/resources to fully implement this policy
- To fully endorse, support and implement the controls outlined in this policy

4.2 Trust executive

The executive lead for digital is the Executive Director of Strategy & Planning / Deputy CEO. The executive lead for information governance is the executive director of finance. They have responsibility to:

- Ensure ALL staff are aware of and adhere to this policy

- Ensure this policy is part of the induction and ongoing awareness process
- Make decisions on disciplinary action required in cases of non-compliance and to empower local IT departments to place immediate orders to legalise software use

4.3 Digital Services Department

- Ensure that auditing / monitoring software is used on an ongoing basis to monitor software licensing compliance and relicense where / when necessary
- Carry out regular audits of software against the list of authorised software within the Divisions of the Trust
- Any non-compliance must be notified to the departmental manager and to the Division Management for immediate action
- Ensure Trust staff are trained in the legal use of software as part of the induction / ongoing training programme
- Ensure appropriate software asset management, to ensure prudent use of Trust funds – for example, ensuring the Trust no longer pays for unused software applications

4.4 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

4.5 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
- Discuss any identified risks and security issues with the service to the appropriate mangers
- Ensure ongoing awareness of policy
- Advise of any requirements for non-standard software
- Report the use of unauthorised software.

5. IMPLEMENTATION

- Disseminate Trust policy on copyright compliance so that employees are made aware of the implications of installing unauthorised software
- Ensure this policy is communicated to all staff via appropriate Trust / Divisions' means, to include via appropriate training programmes, so that employees and contracted third parties can be given information related to their obligations under copyright law.
- Ensure all software deployments have the required information security and information governance oversight – specifically, the completion of a Data Privacy Impact Assessment (DPIA), Cloud Risk Assessment (CRA) and/or Cyber Security Impact Assessment (CSIA)
- Implement approval process
- Implement a Software Asset Register in which all authorised software in use within each Division is recorded
- Software in use within the Trust is audited at regular intervals to ensure each piece of software is correctly licensed.

6. FURTHER INFORMATION

Further information can be obtained from the local Digital Service Desk.

7. REFERENCES

This policy should be read in conjunction with the following documents:

- Information Security Policy
- Anti-Virus Policy
- Internet Use Policy
- Information Governance Policy
- Welsh Health Circular (2017) 025 – Guidance on Cyber Security and Information Governance requirements relating to suppliers and the supply chain

WHC (2017) 025:

WHC 3rd parties holding NHS Wales D