Shropshire Community Health
NHS Trust

Digital Acceptable Use Policy (AUP)

Controlled document

This document is uncontrolled when downloaded or printed.

Author(s) **Owner(s)**	Author: Digital Services Manager Owner: Director of Finance
Version No.	Version 1.0
Approval date	18 September 2025
Review date	September 2028

Document Details	
Title	Digital Acceptable Use Policy (AUP)
Trust Ref No	2530
Local Ref (optional)	
Main points the document covers	Acceptable Use Policy in relation to Digital devices, systems, services and infrastructure
Who is the document aimed at?	This policy is aimed at all staff
Author Owner	Associate Director of Digital Services Director of Finance
Approval process	
Who has been consulted in the development of this policy?	Digital Assurance Group (11/09/2025) Data Security and Protection Assurance Group (18/09/2025)
Approved by (Committee/Director)	Sarah Lloyd – Director of Finance
Approval Date	18 September 2025
Initial Equality Impact Screening	
Full Equality Impact Assessment	
Lead Director	Director of Finance
Category	General
Subcategory	Cyber Security / Information Governance
Review date	September 2028
Distribution	
Who the policy will be distributed to	All staff
Method	Websites, email and Trust Newsletter
Keywords	Cyber; Security; Digital; Mobile;
Document Links	
Required by CQC	Yes – Well Led
Other	

Amendments History		
No	Date	Amendment
1	June 2025	Version: 0.1 Author: Paul Stokes Page: Initial Document - General Responsibilities DSPT CAF requirements (B1.a and B6.a) / best practice and NHSE Cyber Strategy referenced to create this new policy
2	July 2025	Version: 0.2 Author: Paul Stokes Following approval of Digital Security Policy (DSP) Page: An introduction to Acceptable Use Policies Page: Monitoring of Activity and Reporting Reference: Data (Use and Access) Act 2025 (DUAA)
3	11 September 2025	Consultation with DSPAG & SIRO
4	18 September 2025	Approved by DAG & DoF and V1.0 Created
5		
6		
7		
8		
9		

Contents

1. Policy statement

1.1. This policy document forms part of Shropshire Community Health NHS Trust (hereafter described as the Trust) Digital Services Strategy and sets out minimum standards and best practice for ensuring confidentiality, integrity and availability of Information Management and Technology (IM&T) digital assets.

1.2. It complements the requirements of the NHS Data Security and Protection Toolkit (DSPT) and best practice from the Cyber Assessment Framework (CAF) and DoHSC National Cyber Policy.

1.3. Negligent or malicious non-compliance with this policy may be dealt with through the disciplinary process.

2. Related documents, Legal and Regulatory Requirements

2.1. Policies can be found in the Trust's Document Library on Public Website and Staff Zone

- Digital Strategy
- Digital Security Policy (DSP)
- Data Protection Policy
- Records Management & Security Policy
- Information Risk Policy
- Local Registration Authority Policy
- Risk Management Strategy
- Disciplinary Policy & Procedure
- Maintaining High Standards of Performance
- Information Governance Procedures / Standard Operating Procedures

2.2. Legal and Regulatory Requirements – examples:

- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Malicious Communications Act 1998
- Human Rights Act 1998
- Electronic Communications Act 2000
- Freedom of Information Act 2000
- General Data Protection Regulation (UK GDPR) 2018
- Data Protection Act 2018
- The Online Safety Act 2023
- Data (Use and Access) Act 2025 (DUAA)

2.3. Document references

- 'A cyber resilient health and adult social care system in England: cyber security strategy to 2030'
- Cyber Assessment Framework (CAF)-aligned Data Security and Protection Toolkit (DSPT) guidance - NHS England Digital

- National Cyber Security Centre - NCSC.GOV.UK
- A just culture guide for information governance and cyber security - NHS Transformation Directorate
- Williams review into gross negligence manslaughter in healthcare - GOV.UK

3. Purpose

3.1. This document sets out to provide clear Policy statement in relation to the Acceptable Use of the Trust's Digital devices, systems, services and infrastructure.

3.2. Provides reference and signposting for best practice and guidance.

4. Scope

4.1. This Policy entails all personal data held by, or on behalf of The Trust, its processing, storage, handling and usage. Such data includes but is not limited to:

- employee and staff records
- patient/client data and records
- corporate data and records
- personal data relating to volunteers and contractors working with the Trust

4.2. This Policy also entails all Trust Digital Assets such as devices, systems, services and infrastructure owned by, or on behalf of The Trust, its processing, storage, handling and usage. This includes but is not limited to:

- Devices including Servers, PCs, Laptops, Tablets, Mobile Phones
- Software and systems including Microsoft Windows, Teams, Office 365, Anti-Virus, Virtual Private Network (VPN)
- Email, Internet, Printing and Telephony services
- Infrastructure and network access including Corporate & Patient Wi-Fi, Cyber Security

5. Applicability

5.1. All staff that are required to work within the organisation, employed and non-employed, must adhere to this policy and associated policies. Including, but not limited to:

- Employed staff (including Bank staff)
- Volunteers
- Student and Medical Placements
- Allied Healthcare Placements
- Locums
- Agency
- Temporary and Fixed Term contracts
- Third Party Suppliers and Contractors

6. Governance

6.1. The Trust has appropriate management policies, processes and procedures in place to govern its approach to cyber security and the governance of information, systems and networks.

6.2. The Board provides leadership on the management of risk and ensures the approach to risk management is consistently applied as well as determining the information risk appetite for the Trust. The Board is also responsible for setting the Trust's Risk Appetite regarding information and cyber security.

6.3. The Senior Information Risk Owner (SIRO) is the Board's executive level delegate responsible for risk management including oversight of data protection and other aspects of information governance and cyber security.

6.4. The Chief Executive is the Accountable Officer and has overall responsibility for ensuring our compliance with this policy. They have overall responsibility for ensuring that information and cyber security risks are assessed and mitigated to an acceptable level.

6.5. The Associate Director of Digital Services is responsible for the delivery of the Digital Strategy and day-to-day operational monitoring and delivery of the Trust's Digital Services.

6.6. The Data Protection Officer (DPO) is responsible for challenging and advising the Board on data protection to ensure that the Trust remains compliant.

6.7. The Information Governance Manager is responsible for the day-to-day operational monitoring of information governance and information handling.

6.8. The IT Services Manager is responsible for the day-to-day management and operation of the corporate network infrastructure including the secure operation of the network, devices, connections, monitoring, protection and controls.

6.9. All Line Managers are responsible for ensuring that staff with responsibilities set out in this policy can undertake the role sufficiently including training to meet the requirements of this Policy.

6.10. All Staff are responsible for upholding Digital Security requirements, including identifying and managing risk, and understanding/complying with relevant policies, procedures and processes for handling personal data and digital systems appropriate to their role. Staff must immediately report any event or breach affecting digital security or data held by the Trust to their Line Manager.

7. An introduction to Acceptable Use Policies

7.1. Why does the Trust and the NHS have Acceptable Use Policies (AUPs)?

- Alongside a Just Culture, AUPs help protect digital assets, ensuring security, and maintaining a productive work environment.
- They define acceptable and unacceptable behaviours when using digital technology and assets, minimising risks, managing finite resources and clarifying responsibilities for all staff as well as providing sources for education and awareness.

7.2. What is a just culture?

"A just culture considers wider systemic issues where things go wrong, enabling professionals and those operating the system to learn without fear of retribution... in a just culture inadvertent human error, freely admitted, is not normally subject to sanction to encourage reporting of safety issues. In a just culture, investigators principally attempt to understand why failings occurred and how the system led to sub-optimal behaviours. However, a just culture also holds people appropriately to account where there is evidence of gross negligence or deliberate acts."

- Professor Sir Norman Williams Gross negligence manslaughter in healthcare report (June 2018)

- We know that data incidents will happen. We also know that they rarely occur because of one person's actions. Incidents will have deeper root causes and require a broader response
- In the context of Cyber and Information Governance (IG), a just culture is one that supports fairness, openness and learning when addressing identified cyber vulnerabilities, events, attacks, data breaches or near misses, so that people feel confident to speak up rather than fearing blame
- A just culture recognises that most professionals do not come to work to make mistakes or to act maliciously
- It allows for learning to take place to help prevent recurrence
- A key outcome of a just culture is continuous improvement, underpinned by timely reporting, protection of those reporting and learning lessons

7.3. Many digital systems and services you have access to may have their own Acceptable Use Policies (AUPs) including for example, NHSmail and other NHS systems; you must adhere to and follow these AUPs too.

7.4. Malicious or intended violation of AUPs may result in removal of rights to access digital assets, investigation (criminal or otherwise) and/or be subject to the Trust Disciplinary Policy & Procedure and/or Maintaining High Standards of Performance.

8. General Responsibilities

8.1. You must not use digital assets to violate any laws, copyright or regulations of the United Kingdom or other countries. The use of digital assets for illegal activity is forbidden and any illegal activity will be reported to the police. Illegal activity includes, but is not limited to, sending, or receiving material related to paedophilia, terrorism, incitement to racial harassment, stalking, sexual harassment, and treason.

8.2. You must not send any material by Text, Email, Teams, O365 collaboration tool or by any other messaging service that could cause distress or offence to another user. You must not send any material that is obscene, sexually explicit, or pornographic.

8.3. You must also not attempt or access inappropriate, offensive or illegal material such as pornography, items promoting racial or religious hatred and material promoting subversive, terrorist or criminal activities.

8.4. You must not use digital assets to harass other users or groups by sending persistent messages to individuals or distribution lists.

8.5. You must not use any digital asset for private commercial gain. This includes, but is not limited to unsolicited marketing, advertising, and selling goods or services.

8.6. You must not attempt to interfere with the technical components, both hardware and software, of digital assets in any way, for example, disable anti-virus or Multi-Factor Authentication (MFA), remove VPN software, modify the network, or deliberately perform any act that will impair or interrupt the operation of any electronic system or network including Intentional corruption or destruction of data.

8.7. You must not attempt to circumnavigate or avoid the security and governance arrangements that have been put in place to protect digital assets.

8.8. When prompted, you must ensure security updates are installed on digital assets and that they are ‘restarted’ in timely manner. Certain digital assets, for example laptops, must be connected to the corporate network at regular intervals in order to maintain security compliance.

8.9. You must not attempt to or install unauthorised software or services onto digital assets.

8.10. You must not let any unauthorised person access or use digital assets including devices, systems or services

8.11. You must take all reasonable care to ensure that digital asserts such as devices are not subject to loss or damage and kept physically safe.

8.12. You must not connect digital assets to untrusted or unauthorised networks.

8.13. You must not connect untrusted or unauthorised devices to the Trust's network, infrastructure or systems; or attempt to install Trust software or services on to them.

8.14. You must not waste system resource or consume large quantities / volumes of data, for example, by sharing mobile data, viewing streaming services and media content.

8.15. You must not use digital assets to disable or overload any computer system or network. Where excessive account activity is detected, your account could be suspended, without notice, to safeguard the service for all other users.

8.16. When you set up your accounts you must identify yourself honestly, accurately, and completely.

8.17. You must ensure your account passwords follow best practice, are always kept confidential and secure. You should notify your Local Administrator, Information Asset Owner/Administrator or the IT Service Desk if you become aware of any unauthorised access to your accounts or believe your accounts have been compromised.

8.18. You must only input your corporate account passwords into Trust and NHS systems, do not use them for other systems or sites such as social media. You will never be asked for your Windows Logon, NHSmail or any other system password. Do not divulge this information to anyone, even if asked. Applications integrated with NHSmail single sign-on will redirect you to enter your NHSmail credentials via the official NHSmail portal.

8.19. NHSmail is protected by anti-virus and anti-spam software although occasionally, as with any email service, a new virus or spam message may not be immediately detected. If you are unsure of the source of an email or attachment you should leave it unopened and seek advice from the IT Service Desk. If you receive spam messages you should report them to spamreports@nhs.net using the process detailed on Reporting Cyber Threats on the NHSmail support site.

8.20. You must not introduce or forward any virus, malware or any other computer programme that may cause damage to Trust or NHS digital assets.

8.21. It is your responsibility to ensure you are up to date with your local Information Governance and Cyber training.

8.22. Personal use of Internet services is permitted during “non-Trust time”, for example a lunch break. However, your use must still comply with the AUPs, be limited and not interfere with the performance of duties, be excessive or add any significant risk or burden to the Trust’s systems or resources including incurring costs such as accessing or ‘texting’ premium rate services. It is also recommended that you do not conduct personal online banking or purchases using the Trust’s Internet services. The Trust will decide what is considered to be excessive or inappropriate use.

8.23. Line Managers must manage the ‘Joiner, Mover, Leaver’ (JML) process with regards to their staff and digital assets including maintaining a localised inventory of devices held within the team or department, ensuring devices are issued and returned correctly, as well as reviewing system rights for their staff, for example in Microsoft 365.

9. Monitoring of Activity and Reporting

9.1. Digital assets feature an audit log or activity trail. These audit trails provide details of user and device access to systems and services such as information systems, Email, internet, telephony, documents, files etc; and may be used to monitor usage and activity.

9.2. The Trust reserves the right to monitor the use and activity of the devices, systems and services it provides to you.

9.3. Monitoring is routinely undertaken to check performance, efficiency, capacity and appropriate use.

9.4. Incidents and near misses should be raised on the Trust risk management system.

9.5. Concerns and issues should be raised through your Line Manager or the People Directorate.

9.6. Technical queries and advice should be raised through the IT / IG Departments or Information Asset Owner/Administrator.

9.7. You must give consideration when responding to Freedom of Information (FoI) requests around safeguarding national security (section 24 exemption) including details from emails, systems and contracts.

Appendix 1 – Best Practice and Guidance Links

NHS.net Connect (NHSmail) Acceptable Use Policy

NHSmail: Data Retention and Information Management Policy

Reporting Cyber Threats – NHSmail Support

End user organisation acceptable use policy - NHS England Digital

Guide to multi-factor authentication (MFA) policy - NHS England Digital

NCSC lifts lid on three random words password logic - NCSC.GOV.UK

Password policy: updating your approach - NCSC.GOV.UK

Secure sanitisation of storage media - NCSC.GOV.UK

A cyber resilient health and adult social care system in England: cyber security strategy to 2030 - GOV.UK

NHS Data Security and Protection Toolkit (DSPT)

The National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF)

Section 24 – Safeguarding national security | ICO