



IT Acceptable Use Policy

Information reader box

Directorate:

Business Information Services

Publications gateway reference

Document purpose: **Policy**Document name: **IT Acceptable Use Policy**Author: **Gary Ingham, ICT Compliance Manager**Publication date: **21/01/2025**Approving body: **Information Governance Committee**

Target audience: **All IT Users including staff, contractors, consultants, temporary and other workers in NECS, receiving IT services provided by NECS Customers and suppliers where their terms of business with NECS require adherence to the NECS IT Acceptable Use Policy and in so far as the services they receive from NECS are relevant to the policy**

Additional circulation list: **N/A**Description: **Policy**Cross reference: **N/A**Superseded document: **IT Acceptable Use Policy v3.5**Action required: **Compliance with this policy**Timing/deadlines: **N/A****Contact details (for further information)****Gary Ingham, ICT Compliance Manager****Tel: 0191 374 2779****Email: garyingham@nhs.net****Document status**

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

Document information

Staff who become aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives that affect, or could potentially affect policy documents, should advise the sponsoring director as soon as possible, via line management arrangements. The sponsoring director will then consider the need to review the policy or procedure outside of the agreed timescale for revision

Accessible Information Standards

If you require this document in an alternative format, such as easy read, large text, braille or an alternative language please contact NECSU.comms@nhs.net

Document Owner: Joanne O'Donnell	Prepared by: Gary Ingham	First Published: 02/03/2015
	Issue/approval date: 21/01/2025	Version number: 3.6
Status: approved	Next review date: 25/07/2026	Page 1

Contents

1. Policy statement.....	3
2. Introduction	3
3. Scope	3
4. Definitions.....	4
5. Roles and responsibilities	5
6. General Security.....	7
7. Password Management.....	10
8. Account Usage	11
9. Internet & Email.....	13
10. Software Copyright Compliance	15
11. Mobile Devices	15
12. Returning Equipment	16
13. Distribution and implementation.....	16
14. Monitoring.....	17
15. Impact analysis.....	17
16. Associated documentation.....	17
17. References	18
Appendix 1 – Equality impact assessment	19
Governance, ownership and approval.....	21
Appendix 2 – Version control tracker/change log	22

Document Owner: Joanne O'Donnell	Prepared by: Gary Ingham	First Published: 02/03/2015
	Issue/approval date: 21/01/2025	Version number: 3.6
Status: approved	Next review date: 25/07/2026	Page 2

1. Policy statement

The purpose of this Policy is to form a code of conduct for all employees to follow regarding acceptable use of ICT resources and equipment. This Policy will establish acceptable and unacceptable behaviour regarding the use of electronic devices, NECS managed applications, network accounts and information resources at NECS.

NECS IT provides computer devices, networks, and other electronic information systems to meet objectives, goals, and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. This Policy requires users of information assets to comply with applicable legislation and NECS policies, helping to protect the organisation and individual employees against complex legal issues.

2. Introduction

Information security is the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important, valuable asset which must be managed with care.

All NECS Information Communication Technology (ICT) resources and equipment must be used sensibly, professionally, lawfully, and consistently within the bounds of acceptable conduct of business and the duties of each employee's role.

To ensure that information remains secure, is used appropriately and is managed in accordance with relevant regulation and legislation, a code of conduct must be outlined to which all users of ICT resources and equipment must adhere.

This Policy draws on a variety of NHS England and NECS existing policies (see Section 16.1 – Other Related Documents).

3. Scope

This policy applies to:

- NECS staff, customers and suppliers using NECS IT services, to its staff, customers and suppliers
- To all information assets and equipment managed by NECS, and to devices that connect to a NECS network or any applicable NECS site.

Document Owner: Joanne O'Donnell	Prepared by: Gary Ingham	First Published: 02/03/2015
	Issue/approval date: 21/01/2025	Version number: 3.6
Status: approved	Next review date: 25/07/2026	Page 3

- To both fixed essential and agile workers staff, working at a NECS site or remotely, where applicable

All staff are referred to in this Policy as 'IT Users' (see Definitions section 3).

The Policy outlines the general principles to be adhered to, as well as overarching permissible and prohibited activities. Further detail can be found in NECS and NHS England policies; all associated policies are referenced. The user activities addressed by this Policy are:

- Physical security behaviours
- Password management
- General account usage
- Privileged account usage
- Internet use
- Electronic mail use
- Software download and
- Use of mobile devices.

4. Definitions

The following terms are used in this document:

IT Users includes employees, contractors, consultants, temporary and other workers in NECS, suppliers and customers receiving IT services provided by NECS.

Information Systems is the collection of technical and human resources that provide the storage, computing, distribution, and communication of NECS information. This includes all software and hardware required to facilitate any information service.

NECS Network is defined as a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource sharing among a wide range of users.

"NECS Network" is any network that belongs to and is managed by NECS.

Personal Device refers to any electronic device that is not the property of NECS or an affiliated third party.

Personal Use refers to use of IT services and systems that are not in connection with NECS or NHS work.

Mobile device is a general term for any handheld computer or smart phone, that can connect to the internet, e.g., laptops, mobile phones & tablets.

Document Owner: Joanne O'Donnell	Prepared by: Gary Ingham	First Published: 02/03/2015
	Issue/approval date: 21/01/2025	Version number: 3.6
Status: approved	Next review date: 25/07/2026	Page 4

Principle of Least Privilege is the practice of limiting a user's access to information systems to the minimal level possible, whilst enabling the user to fulfil their responsibilities in line with their job role.

Third Parties are organisations that have a requirement to access NECS IT services or systems, such as a system supplier or a customer.

Remote Desktop Services (RDS) is the ability to access another NECS computer/virtual server in a different location.

Virtual Desktop Infrastructure (VDI) allows users to connect to NECS infrastructure and systems from any device.

Use Your Own Device (UYOD) is the name given to using a personal device for accessing the NECS network. The means to accessing the NECS network is via RDS/VDI.

NECS Equipment in the context of this document is equipment managed by NECS on behalf of itself and its customers.

5. Roles and responsibilities

Managing Director

The Managing Director has overall responsibility for ensuring that information is handled appropriately in order to protect information from unauthorised disclosure or misuse.

Director of Business Information Services

The Director of Business Information Services is the sponsoring director for this document and is responsible for ensuring that this Policy remains up to date and that all staff and managers adhere to the processes outlined within this Policy.

Head of Service - Business Information Services

Is responsible for:

- Ensuring a process is followed to confirm this Policy remains up to date and is reviewed regularly
- Ensuring this Policy is available to all employees, including all personnel affiliated with third parties

Document Owner: Joanne O'Donnell	Prepared by: Gary Ingham	First Published: 02/03/2015
	Issue/approval date: 21/01/2025	Version number: 3.6
Status: approved	Next review date: 25/07/2026	Page 5

Infrastructure Security Lead

The Infrastructure Security Lead will:

- Be responsible for updating the privileged user & third-party processes and ensure any changes are reflected in this Policy.

All IT Users

All IT Users are responsible for:

- Compliance with this Policy; IT Users are not to engage in any prohibited activities outlined in this Policy, as stated in section 5.1.3
- Co-operating with the development and implementation of policies and procedures as part of their normal duties and responsibilities
- Identifying the need for a change in policy or procedure as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives, and advising the policy author accordingly
- Identifying training needs in respect of policies and procedures and bringing them to the attention of their line manager
- Attending training / awareness sessions when provided
- Reporting a suspected or confirmed security breach or weakness immediately. Breaches are to be reported by contacting the NECS IT Service Desk and through any other risk management/ incident reporting systems and/or processes
- Report any equipment that has been lost or stolen immediately, including any mobile device e.g., personal laptop or NECS USB stick as used in Use Your Own Device (UYOD) solution.

In the event of leaving the organisation, IT users should not attempt to use any account or access any organisational information.

Document Owner: Joanne O'Donnell	Prepared by: Gary Ingham	First Published: 02/03/2015
	Issue/approval date: 21/01/2025	Version number: 3.6
Status: approved	Next review date: 25/07/2026	Page 6

6. General Security

6.1 Key Principles

6.1.1 Conditions

All IT users accept the following conditions:

- All data and information residing on the NECS networks and associated information systems remains the property of NECS at all times, unless otherwise stated
- NECS retains the right to monitor the use of all NECS information systems. Where NECS considers a significant risk exists to the interests of NECS, customers or affiliated third parties; or where a user is in direct breach of this Policy, NECS may prohibit the use of information systems without warning or consultation
- NECS reserves the right to delete or remove any personal information held on the network if felt to be inappropriate for any reason e.g., personal photographs (see Section 5.1.3 Prohibited Activity).

6.1.2 Acceptable activity

It is permissible for all IT users to:

- Use NECS information systems for personal use, however it is not a right and must be exercised with discretion and moderation. Personal use must not interfere with the performance of duties and those of others. Users further accept that NECS does not accept any liability, in part or whole, for claims arising out of personal use of the NECS information systems or information
- Connect personal devices to the NECS public Wi-Fi, however they will not be permitted to connect to any corporate domain or associated network with the exception of devices being used for UYOD, which would be connected securely via NECS VDI or RDS platforms. In doing so, users must abide by the conditions specified within this Policy. Personal devices can be plugged in, in order only to charge or supply power to a device e.g., mobile phone
- Use a personal mobile phone during business continuity events
- Access an authenticator app on personal mobile phones for work related systems, see section 10.1.3 Mobile Phones

Document Owner: Joanne O'Donnell	Prepared by: Gary Ingham	First Published: 02/03/2015
	Issue/approval date: 21/01/2025	Version number: 3.6
Status: approved	Next review date: 25/07/2026	Page 7

In addition, only customers and suppliers are permitted to:

- Connect a Use Your Own Device (UYOD) to the NECS network, only when using the NECS Virtual Desktop Infrastructure (VDI) or Remote Desktop Services (RDS) platforms either with or without an authorised VDI USB stick.

N.B NECS IT staff are permitted to access UYOD for testing purpose only. Where this occurs, a ticket would be raised within the IT Call Logging System.

NECS reserves the right to withdraw use of its systems including Public Wi-Fi at any time, without prior notice, should the need arise. For example, there is, or it may be likely to have a detrimental effect on the network performance.

6.1.3 Prohibited activity

All IT users are strictly prohibited from:

- Using NECS information systems and information in a manner that will intentionally result in:
 - Breaking the law and/or legal implication.
 - Damage or disruption to the NECS information systems or information.
 - Violation of this Policy.
 - Denying services to others and/or wasting NECS resources.
- Using NECS equipment for the creation, transmission or deliberate receipt of any images, data or other material which is considered offensive
- Accessing information and/or information systems to which they have not been explicitly authorised to access. Any attempt to gain access or circumvent established security mechanisms is strictly prohibited
- Knowingly removing or destroying data; disclosing confidential information; including a false or misleading entry in any non-test data, records, reports or files except in the conduct of approved work duties
- Using NECS IT facilities for commercial activities, advertising or fund raising for organisations not directly connected with NECS unless authorised
- Seeking personal benefit or permitting the unauthorised use of any information acquired, as a result of access to NECS information or their own information
- Copying any data to their personal device, where staff are Using Your Own Device (UYOD) via the VDI or RDS platforms either with or without a NECS USB stick and logging into NECS network.

Document Owner: Joanne O'Donnell	Prepared by: Gary Ingham	First Published: 02/03/2015
	Issue/approval date: 21/01/2025	Version number: 3.6
Status: approved	Next review date: 25/07/2026	Page 8

In addition, NECS staff are also prohibited from:

- Using a personal mobile device (e.g., mobile phone/laptop) for work purpose (except as outlined in 5.1.2)

NECS monitor the usage of all NECS issued mobile phones. If personal usage is deemed excessive this may be investigated further and disciplinary action may be taken. NECS hold the final decision on 'excessive' use.

In the event of Cyber Attack, NECS will not respond to ransom demands. Some of the main reasons for this are as follows:

- NECS has no legal powers to use public money in this way.
- There is no guarantee that paying a ransom will get access to the data or computer.
- The organisation is likely to be at greater risk of being targeted in the future.
- A computer will still be infected.

6.2 Physical Access – NECS Sites

All IT Users must be able to identify themselves at all times (e.g., wearing ID badges at all times), in the interests of maintaining the integrity of information and information systems. All IT users are responsible for challenging anyone suspicious. Anyone unable to identify themselves should be treated as unauthorised individuals and should be escorted off site if it is safe to do so.

6.3 Clear Desk

6.3.1 User Responsibilities

All IT Users must ensure that when leaving their desk or work environment, desks are clear of all confidential documentation and portable media devices (with the exception of laptops). Confidential documents should either be destroyed or stored in a secure location. Media devices should either be stored away in a secure location or and cleared if the data is no longer required.

Documents must not be left at printers and should be collected immediately following printing.

Visual controls, graphical representations, team-based notices and information may remain on display during out of office hours providing that the information is not confidential or commercially sensitive. Confidential or commercially sensitive information must not be removed from site, unless authorised to do so, and should be stored in a secure location.

Document Owner: Joanne O'Donnell	Prepared by: Gary Ingham	First Published: 02/03/2015
	Issue/approval date: 21/01/2025	Version number: 3.6
Status: approved	Next review date: 25/07/2026	Page 9

When working away from the normal place of work and using either NECS provided equipment or Using Your Own Device (UYOD), users must protect their screen to prevent unauthorised people from viewing work related information (shoulder surfing) taking place. When a machine is not in use, the computer screen must be locked at all times.

5.3.2 NECS Responsibilities

NECS will provide a method of sensitive document disposal and secure storage facilities. Other organisations receiving IT services from NECS have a responsibility to provide the same or equivalent facilities.

Periodic inspections may be carried out by NECS IG or their representatives, without prior notice, to ensure compliance with the clear desk requirements.

6.4 Computer & Printer Locking

All IT Users must lock their computer screen, including those who are Using Your Own Device (UYOD), when away from their desk or work environment. This can be achieved using the keyboard by pressing 'Ctrl' 'Alt' & 'Del' together or by pressing the 'Windows key' & 'L' together. IT Users must not wait for the auto screensaver to activate.

All devices must be powered down when no longer in use to allow encryption and software updates to operate effectively. In the event that a device is compromised, where an IT User had left a device turned on, then that individual will be held wholly accountable for any data loss.

Print lock facilities (code to retrieve printing) should be used where available.

7. Password Management

All IT Users must follow good security practices in the selection and use of passwords, including:

- Not writing down passwords unless absolutely necessary (where necessary, passwords must be kept in locked drawer or carried separately from computer)
- Not disclosing passwords to any other person or organisation
- Ensuring passwords are changed when prompted to do so
- Changing passwords immediately if there are suspicions it has been compromised
- Not basing passwords on anything that could be easily guessed by another e.g., users own name, children or pets names or "Password1"

Document Owner: Joanne O'Donnell	Prepared by: Gary Ingham	First Published: 02/03/2015
	Issue/approval date: 21/01/2025	Version number: 3.6
Status: approved	Next review date: 25/07/2026	Page 10

- Updating passwords immediately if informed by NECS IT Security that it is classed as 'weak', even though it meets the password security requirements e.g., Password2!
- Password reuse to access multiple systems/accounts is not encouraged and is strictly prohibited for passwords used to access highly privileged accounts

Monitoring is in place by NECS IT Security Team, which may require a change of password, should the above not be adhered to.

8. Account Usage

8.1 Standard User Accounts

NECS does not permit the sharing of account details, including passwords.

Each IT User must have an individual account; the owner of that account has full responsibility. All users should have a standard account for daily activities regardless of job role. The user must not share logon credentials with any other user or organisation.

If an IT User suspects that their logon credentials have been compromised, they should raise an incident with the NECS IT Service Desk immediately.

Should a user require NECS technical support, it is the IT User's responsibility to confirm the identity of any user accessing their account, to carry out any support duties. If a user has any concerns, they should immediately raise an incident through the NECS IT Service Desk.

8.2 Privileged User Accounts

In accordance with the 'principle of least privilege' and NHS Digitals Data Security and Protection Toolkit, privileged accounts are only to be used when absolutely necessary to complete assigned job duties; IT staff are prohibited from using their privileged accounts for high-risk activities that do not require elevated access, such as reading emails or browsing the internet. All other job duties should be completed using a standard user account to guard against inadvertent administration errors and unintentional software download.

IT Users who have been granted Privileged user status will adhere to the NECS IT Change Management Procedures and will not intentionally bypass the change management process to implement any changes. Intentional unauthorised changes may be subject to disciplinary action, termination of contract or legal action.

Document Owner: Joanne O'Donnell	Prepared by: Gary Ingham	First Published: 02/03/2015
	Issue/approval date: 21/01/2025	Version number: 3.6
Status: approved	Next review date: 25/07/2026	Page 11

In the event of inadvertent administration errors or malicious software being downloaded, the user must inform their line manager and IT Security immediately. A supporting incident should be raised within the IT Service Management System.

If heightened privileges are no longer required, the user is to inform the NECS IT Service Desk so that permissions can be revoked.

NECS reserves the right to downgrade any privileges if this is no longer required, or in the event of misuse.

No privileged accounts shall be used on Using Your Own Device (UYOD).

8.3 Third Party Accounts

8.3.1 Terms and conditions

In addition to the other conditions outlined in this Policy (Including Standard User Accounts 7.1) the following conditions must be adhered to:

- The third party will be held responsible for any unauthorised use of the IT account.
- The third party is not permitted to share the logon credentials with any person outside of the company or permit any other person or entity outside of the company to access information using the account.
- The third party must take all precautions to prevent against malicious access and/or malware software and viruses and not knowingly download any suspect files or software.
- Upon completion of the project role or the contract, the third party will inform NECS, and the account will be disabled. NECS requires formal notification with a minimum of 5 working days' notice for future access. This request will be subject to NECS Change Management Procedures and must be authorised prior to account reactivation.
- Account use should be restricted to nominated individuals only. Generic use of the account is permitted amongst these individuals only. Should any nominated individual's employment be terminated, the account must be suspended, and the password must be changed.
- Misuse of third-party accounts will lead to the immediate suspension of the account and possible investigation. Confirmed misuse could result in the withdrawal or termination of any standing contract and may lead to legal action by NECS.

8.3.2 Third party use

IT users accessing a third-party account (suppliers and customers) must:

- Adhere to all elements of this Policy

Document Owner: Joanne O'Donnell	Prepared by: Gary Ingham	First Published: 02/03/2015
	Issue/approval date: 21/01/2025	Version number: 3.6
Status: approved	Next review date: 25/07/2026	Page 12

- Only use the account to fulfil agreed contractual requirements
- Not download software without the prior permission of NECS. This must be formally documented prior to any download taking place.

8.4 Account Inactivity

For accounts to remain active, passwords must be changed in line with the 'Information Governance Fact Sheet 14 Information Security at Work and in the Home' and **IT** users must ensure that they do not leave an account unused for a period of 60 days or more, as the account will be disabled. To prevent the account from being automatically disabled, a user should logon to their account prior to the commencement of the 60th day since their last logon.

Once an account has been disabled due to inactivity, the **IT** user must contact the NECS IT Service Desk to validate their identity. Line Manager authorisation will also be required to re-enable the account.

8.5 Deletion of Accounts & Associated Information

For staff from organisations that are also provided with NECS Human Resources support, NECS IT will be informed by NECS People Services of any IT users leaving the organisation and/or changing job role, at which point the account will be disabled and/or permissions amended as appropriate.

Organisations that are not provided with NECS People Services support must inform the NECS IT Service Desk of IT users leaving or changing role. This is particularly important for IT users who are Using Your Own Device (UYOD), so that their account and access to the NECS network can be disabled accordingly. If they were issued with a VDI USB stick, then this equipment must be returned to NECS IT.

Accounts that have been inactive for a period of 12 months will be deleted. It is the responsibility of the IT User and their line manager to ensure that all information associated with the account is transferred to another appropriate location (e.g., a shared network folder), prior to the IT User leaving an organisation, as it will not be able to be retrieved at a later date.

9. Internet & Email

9.1 Internet Acceptable Use

Document Owner: Joanne O'Donnell	Prepared by: Gary Ingham	First Published: 02/03/2015
	Issue/approval date: 21/01/2025	Version number: 3.6
Status: approved	Next review date: 25/07/2026	Page 13

No IT User is permitted to access, display, or download from Internet sites, that hold inappropriate/adult content such as pornography, ethnic hate inducing content, or materials that can be construed as rude, intolerant or demeaning.

In order to prevent exposure to inappropriate/adult content, technical blocks are in place wherever possible. However, it is considered a breach to access such material and is subject to disciplinary action.

The use of bulletin boards and chat forums is only permitted for business purposes.

All IT Users are personally responsible for the content they publish on blogs, wikis or any other form of user-generated media (social media sites e.g., Facebook, Twitter). All IT Users must make it clear that they are not speaking on behalf of NECS, unless authorised to do so.

IT Users must never broadcast content damaging to NECS or their customers and will be held wholly accountable for any such activity.

All IT Users must not use social media in any way to attack or abuse colleagues.

IT Users must respect copyright, fair use, data protection, defamation, and financial disclosure laws. Never reveal confidential information (including conversations) about patients, staff, or the organisation. Never post any information that can be used to identify a patient's identity or health condition in any way.

NECS reserves the right to monitor internet and email use.

9.2 Transmission of electronic data (Including Email)

Email must be primarily used for business use. Occasional and reasonable personal use is permitted, provided such use does not interfere with the performance of duties and does not conflict with the NHS England policies, procedures and contract of employment.

Any confidential data transferred electronically should be done so via a secure method. Shared drives; secure file transfer; and encrypted portable media are all acceptable ways of securely transferring data.

All electronic mail containing information deemed patient identifiable or otherwise confidential must be sent via a secure method. If NHS Mail to NHS Mail, the method is considered secure. If sent to external email addresses, the sensitive information should be encrypted.

All passwords and log in details for email systems must be kept confidential.

IT Users should not intentionally create, initiate, and/or participate in SPAM mail.

NECS reserves the right to monitor and control access to shared drives and removable portable media.

Document Owner: Joanne O'Donnell	Prepared by: Gary Ingham	First Published: 02/03/2015
	Issue/approval date: 21/01/2025	Version number: 3.6
Status: approved	Next review date: 25/07/2026	Page 14

10. Software Copyright Compliance

IT Users are strictly prohibited from installing software (except NECS in-house developed software) on their NECS device, unless approved and within the conduct of work duties.

All software must be officially requested and authorised via a service request raised in the IT Call Logging System. Any software downloaded without permission could result in disciplinary action/ termination of contract/ or legal action.

No IT user is allowed to make unauthorised copies of any software under any circumstances.

NECS reserve the right to remove any unauthorised software from NECS managed IT equipment.

Staff who are Using Your Own Device (UYOD) are responsible for their own licencing requirements for their own device. e.g., Windows Licence. Any licence required for the VDI or RDS platforms or the VDI USB stick will be the responsibility of NECS.

11. Mobile Devices

11.1 Mobile Devices

11.1.1 Laptops/Desktop PCs

Mobile devices owned by NECS must only be used to access the Internet (adhering with section 8 - Transmission of electronic data, above), NHS Mail, and the NECS network through the applicable remote access software.

Mobile devices should only be used temporarily to store data.

Mobile devices should not be switched off for long periods of time, when not in use, to allow encryption to be effective and security updates to be applied.

If a personal device is being used for UYOD either with or without a NECS VDI USB stick for the sole purpose of accessing the NECS network, then this must be from a home broadband and not public Wi-Fi e.g., coffee shop where Wireless Access Points are more likely to be compromised.

11.1.2 USB drives

Personal USB drives

Use of personal memory sticks/ pen drives is not permitted and must be NECS supplied encrypted memory sticks to be compatible with NECS ICT resources.

Document Owner: Joanne O'Donnell	Prepared by: Gary Ingham	First Published: 02/03/2015
	Issue/approval date: 21/01/2025	Version number: 3.6
Status: approved	Next review date: 25/07/2026	Page 15

NECS supplied encrypted USB drives

NECS USB drives are permitted for the temporary transfer of work-related data only.

NECS supplied unencrypted USB drives

It should be noted that an exception to this is for work related tasks e.g., device imaging etc, whereby NECS IT unencrypted USB drives are required. All user data must be copied onto an encrypted drive and deleted when no longer needed.

11.1.3 Mobile Phones

If using a personal mobile phone in NECS offices, the individual may use the NECS guest Wi-Fi hot spot only; access to corporate Wi-Fi is not permitted (see 5.1.3 Prohibited activity). Use of NECS guest Wi-Fi services is not guaranteed and access to some services may be restricted.

The use of NECS provisioned mobile phones must only be used as a Wi-Fi hot spot when the owner is travelling or working from a customer site and no Wi-Fi is available. They must not be used as a replacement for lack of suitable broadband connectivity while working from home. Short term emergency usage is permitted, such as during a power cut, but must be discussed and agreed with line management.

A personal mobile phone may be used for authentication purposes e.g. the authenticator app, see 5.1.3 Prohibited activity.

NECS IT reserve the right to impose bandwidth limits on mobile phone data usage to ensure best use of available budgets and that pre-agreed commercial arrangement with network providers are adhered.

Further information around mobile devices, can be found in the NECS Mobile Device and Remote Working Procedure.

12. Returning Equipment

IT Users must return all NECS owned IT equipment to the NECS IT Department prior to termination of their employment. This also includes NECS VDI USB stick used for UYOD.

13. Distribution and implementation

All directors and managers are responsible for ensuring that relevant staff within their own directorates and departments have read and understood this Policy and are competent to carry out their duties in accordance with this Policy.

This Policy will be available to all staff for use in relation to access control management, via the NECS Intranet and NECS Internet <https://www.necsu.nhs.uk/who-we-are/our-policies/>

Document Owner: Joanne O'Donnell	Prepared by: Gary Ingham	First Published: 02/03/2015
	Issue/approval date: 21/01/2025	Version number: 3.6
Status: approved	Next review date: 25/07/2026	Page 16

It will be the responsibility of the Information Governance Committee to support the implementation of this Policy across NECS.

All staff will be notified of a new or revised document via a Team Talk bulletin.

14. Monitoring

The monitoring of this Policy will be ensured by the Information Governance Committee Work Programme.

15. Impact analysis

As part of the development of this policy, its impact on equality has been assessed. The outcome of the assessment should be summarised here.

The Equality Impact Assessment Screening Assessment can be found at Appendix 1.

16. Associated documentation

16.1 Other related documents

This Policy is written in conjunction with the following policy documents:

NECS Staff must adhere to all policies outlined below.

- NECS IT Access Control Policy
- NECS IT Change Management Procedures
- NHS England Internet & Email Policy
- NECS Mobile Device and Remote Working Procedure
- NHS England Information Governance Policy
- NHS England Information Security Policy
- NHS England Social Media and Attributed Digital content Policy
- NHS England Health and Safety Policy
- NHS England Standards of Business Conduct Policy
- NHS Records Management Code of Practice 2021
- NHSE Corporate Document and Records Management Policy
- NHSE Confidentiality Policy

16.2 Legislation and statutory requirements

This Policy is written in adherence with the following requirements:

Document Owner: Joanne O'Donnell	Prepared by: Gary Ingham	First Published: 02/03/2015
	Issue/approval date: 21/01/2025	Version number: 3.6
Status: approved	Next review date: 25/07/2026	Page 17

- ISO 27001 Information Security
- NHSD Data Security and Protection Toolkit
- Data Protection Act 2018/GDPR
- Computer Misuse Act 1990 (CMA)
- Copyright, Design & Patents Act 1988
- Obscene Publications Act 1959
- Criminal Justice Act 1988
- Criminal Justice and Public Order Act 1994
- Protection from Harassment Act 1997
- Regulation of Investigatory Powers Act 2000
- Race Relations Act 1976
- Telecommunications Act 1984
- Human Rights Act 1998
- Electronic Communications Act 2000
- Common Law Duty of Confidentiality
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Malicious Communications Act 1988
- Trade Marks Act 1994
- Freedom of Information Act 2000
- Terrorism Acts
- Protection of Children Act 1978

17. References

None.

Document Owner: Joanne O'Donnell	Prepared by: Gary Ingham	First Published: 02/03/2015
	Issue/approval date: 21/01/2025	Version number: 3.6
Status: approved	Next review date: 25/07/2026	Page 18

Appendix 1 – Equality impact assessment

Initial screening assessment (Step 1)

As a public body organisation we need to ensure that all our current and proposed strategies, policies, services and functions, have given proper consideration to equality, diversity and inclusion, do not aid barriers to access or generate discrimination against any protected groups under the Equality Act 2010 (Age, Disability, Gender Reassignment, Pregnancy and Maternity, Race, Religion/Belief, Sex, Sexual Orientation, Marriage and Civil Partnership).

This screening determines relevance for all new and revised strategies, policies, projects, service reviews and functions.

Completed at the earliest opportunity it will help to determine:

- The relevance of proposals and decisions to equality, diversity, cohesion and integration.
- Whether or not equality and diversity is being/has already been considered for due regard to the Equality Act 2010 and the Public Sector Equality Duty (PSED).
- Whether or not it is necessary to carry out a full Equality Impact Assessment.

Name(s) and role(s) of person completing this assessment:

Name: Gary Ingham

Job Title: ICT Compliance Manager.

Organisation: NECS

Title of the service/project or policy: NECS IT Acceptable Use Policy

Is this a;

Strategy / Policy ☒ **Service Review** ☐ **Project** ☐

Other [Click here to enter text.](#)

What are the aim(s) and objectives of the service, project or policy:

[Click here to enter text.](#)

Document Owner: Joanne O'Donnell	Prepared by: Gary Ingham	First Published: 02/03/2015
	Issue/approval date: 21/01/2025	Version number: 3.6
Status: approved	Next review date: 25/07/2026	Page 19

Who will the project/service /policy / decision impact?

(Consider the actual and potential impact)

- **Staff** ☒
- **Service User / Patients** ☐
- **Other Public Sector Organisations** ☐
- **Voluntary / Community groups / Trade Unions** ☐
- **Others, please specify** [Click here to enter text.](#)

Questions	Yes	No
Could there be an existing or potential negative impact on any of the protected characteristic groups?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Has there been or likely to be any staff/patient/public concerns?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Could this piece of work affect how our services, commissioning or procurement activities are organised, provided, located and by whom?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Could this piece of work affect the workforce or employment practices?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Does the piece of work involve or have a negative impact on: <ul style="list-style-type: none"> • Eliminating unlawful discrimination, victimisation and harassment • Advancing quality of opportunity • Fostering good relations between protected and non-protected groups in either the workforce or community 	<input type="checkbox"/>	<input checked="" type="checkbox"/>

If you have answered no to the above and conclude that there will not be a detrimental impact on any equality group caused by the proposed policy/project/service change, please state how you have reached that conclusion below:

The review of the questions above show that there is no impact. The Policy applies equally to all staff, customer and supplier groups as stated in this Policy

If you have answered yes to any of the above, please now complete the

‘STEP 2 Equality Impact Assessment’ document

Document Owner: Joanne O'Donnell	Prepared by: Gary Ingham	First Published: 02/03/2015
	Issue/approval date: 21/01/2025	Version number: 3.6
Status: approved	Next review date: 25/07/2026	Page 20

Accessible Information Standard	Yes	No
Please acknowledge you have considered the requirements of the Accessible Information Standard when communicating with staff and patients. https://www.england.nhs.uk/wp-content/uploads/2017/10/accessible-info-standard-overview-2017-18.pdf	<input checked="" type="checkbox"/>	<input type="checkbox"/>
If any of the above have not been implemented, please state the reason: N/A		

Governance, ownership and approval

Please state here who has approved the actions and outcomes of the screening		
Name	Job title	Date
Gary Ingham	ICT Compliance Manager	14/01/2025

Publishing

This screening document will act as evidence that due regard to the Equality Act 2010 and the Public Sector Equality Duty (PSED) has been given.

If you are not completing 'STEP 2 - Equality Impact Assessment' this screening document will need to be approved and published alongside your documentation.

Please send a copy of this screening documentation to:
NECSU.Equality@nhs.net **for audit purposes.**

Document Owner: Joanne O'Donnell	Prepared by: Gary Ingham	First Published: 02/03/2015
	Issue/approval date: 21/01/2025	Version number: 3.6
Status: approved	Next review date: 25/07/2026	Page 21

Appendix 2 – Version control tracker/change log

Guidance on version control is set out in appendix B of NECS information labelling and classification procedure, which can be found on NECSUS.

Version Number	Date	Author Title	Status	Section Page Overview/Changes
3.5	04/07/2024	Gary Ingham	DRAFT	<p>CE+ Requirement – Policy has been updated to stipulate the prohibit use of personal mobile devices or permitted if managed within MDM.</p> <p>ISO27001 Internal Audit identified the labelling/classifications of this Policy was incorrect – (was labelled Commercially Sensitive, however this is available to customers on the NECS public facing website - Policy updated</p> <p>ISO27001 Gap Analysis identified the Policy is too vague on Internet Acceptable Use – Policy updated (section 8.1 Internet Acceptable Use)</p> <p>Other minor changes which include the removal of names i.e. Safestick</p> <p>To be approved at IGC 04/07/2024</p>
3.5	13/08/2024	Gary Ingham	Approved	Approved by NECS IGC and Executive Team
3.6	21/01/2025	Gary Ingham	Approved	<p>Section 10.1.1 updated to advise mobile devices should only be used temporarily to store data.</p> <p>Added Returning Equipment as a separate section (11) and updated</p>

Document Owner: Joanne O'Donnell	Prepared by: Gary Ingham	First Published: 02/03/2015
	Issue/approval date: 21/01/2025	Version number: 3.6
Status: approved	Next review date: 25/07/2026	Page 22

Version Number	Date	Author Title	Status	Section Page Overview/Changes
				Full document review Update to document owner Minor change approved at IGC

© NHS England
Developed by NHS NECS

First published March 2015
Published in electronic format only

Document Owner: Joanne O'Donnell	Prepared by: Gary Ingham	First Published: 02/03/2015
	Issue/approval date: 21/01/2025	Version number: 3.6
Status: approved	Next review date: 25/07/2026	Page 23