A care system support organisation

NHS

IT Acceptable Use Policy

Information Reader Box

Directorate	
Business Information Services	
Publications Gateway Reference	
Document Purpose	Policy
Document Name	IT Acceptable Use Policy
Author	Alison Emslie, ICT Compliance Manager Tel: 0191 217 2878 Email: alison.emslie@nhs.net
Publication Date	July 2022
Approving Body	NECS Executive Group
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Superseded Document	IT Acceptable Use Policy v3.2
Action Required	Compliance
Timing/Deadlines	n/a

Contact Details (for further information)

Alison Emslie, ICT Compliance manager
Tel: 0191 217 2878
Email:alison.emslie@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.

Contents

1 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).

1.1 Status

This Policy is an IT policy.

2 Purpose and Scope

2.1 Purpose

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 missions, 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.

2.2 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.
- To both fixed and agile 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.

3 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.

Offensive Material refers to any material that is designed or likely to cause offence or needless anxiety, or is abusive, sexist, racist, defamatory, obscene or indecent. NECS holds the final decision on 'offensive' material or prohibited activities.

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.

4 Duties and responsibilities

4.1 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.

4.2 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.

4.3 Infrastructure Security Lead

The Infrastructure Security Lead will:

- Be responsible for ensuring that a process is followed to confirm this Policy remains up to date and is reviewed regularly
- Be responsible for ensuring that this Policy is available to all employees, including all personnel affiliated with third parties
- Be responsible for updating the privileged user & third-party processes and updating this Policy.

4.4 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
- 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.

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

- 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 Safeboot stick as used in Use Your Own Device (UYOD) solution.

5 General Security

5.1 Key Principles

5.1.1 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).

5.1.2 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 a Use Your Own Device (UYOD) to the NECS network, only when using the NECS VDI platform either with or without an authorised VDI USB Safeboot stick.

- 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 platform. 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.

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.

5.1.3 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.

- Where staff are Using Your Own Device (UYOD) via the VDI platform either with or without a NECS USB Safeboot stick and logging into NECS network they are prohibited from copying any data to their personal device.

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.

5.2 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.

5.3 Clear Desk

5.3.1 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 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 and should be stored in a secure location.

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 “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 IT Security or their representatives, without prior notice, to ensure compliance with the clear desk requirements.

5.4 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.

6 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 prompt 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”
- 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!

7 Account Usage

7.1 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 of the account'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.

7.2 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 inadvertent 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.

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 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).

7.3 Third Party Accounts

7.3.1 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 ITIL 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.

7.3.2 Third party use

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

- Adhere to all elements of this Policy
- 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.

7.4 Account Inactivity

For accounts to remain active, passwords must be changed in line with the NHS Password Management guidance and 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 user must contact the NECS IT Service Desk to validate their identity. Line Manager authorisation will also be required to re-enable the account.

7.5 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 Human Resources 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 Human Resources support must inform NECS IT of staff leaving or changing role. This is particularly important for staff 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 Safeboot 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.

8 Internet & Email

8.1 Internet Acceptable Use

No IT User is permitted to access, display, or download from Internet sites, that hold offensive material; to do so is considered to be a serious breach of security.

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, libel 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.

8.2 Transmission of electronic data (Including Email)

Email must be primarily for business use. Occasional and reasonable 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.

9 Software Copyright Compliance

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 to IT Security. Any software downloaded without permission could result in disciplinary action/ termination of contract/ or legal action.

No 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 platform or the VDI USB Safeboot stick will be the responsibility of NECS.

10 Mobile Devices

10.1 Mobile Devices

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.

No data should be stored locally on the mobile device.

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

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.

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. 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.

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.

If a personal device is being used for Use Your Own Device (UYOD) either with or without a NECS VDI USB Safeboot 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.

10.2 Returning Equipment

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

11 Distribution and implementation

This Policy will be available to IT Users receiving IT Services from NECS.

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

12 Enforcement

Any user found to be in breach of this Policy will be subject to disciplinary or other relevant action which may result in the suspension of the account, dismissal, termination of contracts or legal action.

13 Training Implications

Training should be commensurate to ensure that all IT Users have an acceptable understanding of this Policy.

14 Monitoring, Review and Archiving

14.1 Monitoring

The Director of Business Information Services, as sponsor director, will agree with the Infrastructure Security Manager a method for monitoring the dissemination and implementation of this Policy. Monitoring information will be recorded in the policy database.

14.2 Review

The sponsoring director will ensure that this Policy is reviewed in accordance with the timescale specified at the time of approval. **No policy or procedure will remain operational for a period exceeding two years without a review taking place.**

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

NB: If the review consists of a change to an appendix or procedure document, approval may be given by the sponsor director and a revised document may be issued. Review to the main body of the policy must always follow the original approval process.

14.3 Archiving

Corporate Governance Lead will ensure that archived copies of superseded policy documents are retained in accordance with Records Management Code of Practice for Health and Social Care 2016.

15 Equality Analysis

This document forms part of NECS' commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities.

As part of its development this document and its impact on equality has been analysed and no detriment identified. The analysis follows 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:

- IS0 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

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
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:
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.

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** The policy also applies to 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.

Questions	Yes	No
Could there be an existing or potential negative impact on any of the protected characteristic groups?	☐	☒
Has there been or likely to be any staff/patient/public concerns?	☐	☒
Could this piece of work affect how our services, commissioning or procurement activities are organised, provided, located and by whom?	☐	☒
Could this piece of work affect the workforce or employment practices?	☐	☒
Does the piece of work involve or have a negative impact on: • 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	☐	☒

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 the Policy.

If you have answered yes to any of the above, please now complete the 'STEP 2 Equality Impact Assessment' document

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	☐	☐
If any of the above have not been implemented, please state the reason: Click here to enter text.		

Governance, ownership and approval

Please state here who has approved the actions and outcomes of the screening		
Name	**Job title**	**Date**
Alison Emslie	ICT Compliance Manager	02/03/2021

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.**