Doncaster and Bassetlaw Teaching Hospitals
NHS Foundation Trust

Acceptable Use Policy – IT Systems

Did you print this document yourself?

The Trust discourages the retention of hard copies of policies and can only guarantee that the policy on the Trust website is the most up-to-date version. **If, for exceptional reasons, you need to print a policy off, <u>it is only valid for 24 hours.</u>**

Executive Sponsor(s)	Chief Information Officer (CIO) & Senior Information Risk Owner (SIRO)
Date written	28/07/2022
Author/reviewer: (this version)	Roy Underwood – Information Governance Manager David Linacre – Head of Digital Jerome Boniface - IT Security Manager
Date written/revised:	June 2023
Approved By	IG Committee
Date of approval	26th June 2023
Date issued	July 2023
Next review date	July 2025
Target audience:	Trust-wide & 3rd Parties

Amendment Form

Version	Date	Brief Summary of Changes	Author
Version 1	July 2023	This is a new policy – Please read in full	IT Security Manager

Contents

Page No.

1. INTRODUCTION

Information and information systems are important assets, and it is essential to take all the necessary steps to ensure that they are always protected, additionally, to ensure that the systems are available and accurate to support safe and secure Patient care via the Doncaster and Bassetlaw Teaching Hospitals NHS Foundation Trust IT systems.

This document describes the responsibilities and provides guidance around the acceptable use of IT hardware software and Information assets of Doncaster and Bassetlaw Teaching Hospitals NHS Foundation Trust (henceforth referred to as either "DBTH" or "The Trust").

Non-compliance with the clauses in this document may result in disciplinary action.

If users require more information to clarify an obligation listed here, they should contact the Trust Head of Information Governance (IG).

2. PURPOSE

The purpose of this policy is to inform users of their obligations covering all activity on DBTH provided IT equipment, networks and data sources including mobile phones.

The policy covers the following areas for acceptable use:

- Responsibilities and use of IT assets
- Use of e-mail and internet
- Network access (including user accounts and password security)
- Guest Wi-Fi
- Mobile device usage
- Data Storage
- Remote access

This policy applies to those members of staff that are directly employed by the Trust and for whom the Trust has legal responsibility. For those staff covered by a letter of authority/contract or work experience the organisation's policies are also applicable whilst undertaking duties for or on behalf of the DBTH. Further, this policy applies to all third parties and others authorised to undertake work on behalf of the DBTH. For the purposes of this policy the aforementioned will be referred to as users throughout the remainder of this document.

3. GENERAL PRINCIPLES

To protect users and DBTH Trust when using the Trust IT equipment for the Trust business or personal purposes and to ensure proper, secure conduct of business and operations, it is important that any use of this equipment MUST comply with the following principles:

- It does not break the law
- It does not risk bringing the Trust into disrepute or placing it in a position of liability
- It does not violate any provision set out in this or any other policies
- It does not cause damage or disruption to the Trust systems or business.

All data and information residing on the Trust information systems remains the property of the Trust at all times, unless otherwise stated.

Users accept that personal use of the Trust information systems is not a right and must be exercised with discretion and moderation. Users further accept the Trust will not accept any liability, in part of whole, for any liability for claims arising out of personal use of the Trust information systems or Trust information

The Trust retains the right to:

- monitor the use of its information systems for the purpose of protecting legitimate concerns
- prohibit personal use of information systems without warning or consultation whether collectively, where evidence points to a risk to the Trust and/or constituent businesses, or individually where evidence points to a breach of this or any other Trust or NHS policy.

Users are not permitted to access, attempt to access, circumvent, attempt or cause to circumvent, established security mechanisms or controls to view, modify, delete or transmit information and/or information systems to which they have not given explicit access or authorisation.

4. DUTIES AND RESPONSIBILITIES

Overall accountability for procedural documents across the organisation lies with the Head of Information Governance who has overall responsibility for establishing and maintaining an effective document management system, for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents.

Overall responsibility for the Acceptable Use of IT policy lies with the Trust Head of Digital Operations and Cyber Security who has delegated responsibility for managing the implementation of the policy and associated procedural documents.

The Trust Information Governance Lead will provide IG advice and guidance and support The Trust management where applicable.

Staff will receive instruction and direction regarding the policy from a number of sources:

- policy/strategy and procedure manuals
- line Manager
- other communication method (e.g. team brief / Buzz articles); and intranet

5. COMPUTER MISUSE

All users are responsible for personal, legal, and ethical responsibility for maintaining the security, confidentiality, integrity, and availability at all times of the relevant IT systems. This includes the applications and data held within them.

Specifically, in terms of IT access, users must ensure that they do not personally attempt to gain unauthorised, malicious and/or illegal electronic access to any of the Trust IT systems, resources, or materials.

Specifically, users have a duty of care towards ensuring:

- The prevention of unauthorised, malicious and/or illegal access by any individual to any of the Trust IT systems, resources and/or materials.
- The prevention of any individual from using any of the Trust IT systems, resources and/or materials in order to commit or facilitate an offence as defined within the law and/or as advocated within the Trust documented policies and procedures
- The prevention of unauthorised, malicious and/or illegal modification to, or corruption of, any of the Trust IT systems, resources and/or materials.
- Unauthorised disclosure of personal confidential information.

Users must report to their Line Manager or to IT ServiceDesk of any suspicions relating to computer misuse that include:

- Any individual attempting to gain access or exceed the access and/or privilege levels to any of the Trust IT application systems, resources, or materials for which they do not have direct authorisation.
- Any individual attempting to use another user's member's ID and password to gain access to any of the Trust IT application systems, resources, or materials.

Users must ensure that they do not personally undertake - and prevent wherever possible by reporting suspicions regarding – illegal electronic activities which attempt to utilise, modify or adapt any of the Trust IT systems, resources and / or materials in order to perform activities or functions that represent a breach of national NHS policy and / or UK law, and that are therefore in direct contravention of organisation policies and protocols, including but not limited to:

- Proactively sharing account and password details
- Attempting to use the Trust Internet and/or email system to receive and / or transmit pornographic, violent, or sexual images.
- Attempting to use the Trust network and/or resources to duplicate copyright protected software for personal and/or financial gain.
- Attempting to use the Trust network and/or resources to develop, create or perpetuate any form of computer virus or malicious software, including the purposeful uploading or transmission of a known computer virus or item of malicious software to others, whether internal or external to the organisation.

Users must ensure that they do not personally undertake - and prevent wherever possible by reporting suspicions regarding - potential corruption of the Trust IT assets by any attempt to subvert, amend, modify or otherwise inappropriately compromise or affect, any of the Trust's IT application systems resources and/or materials, including:

- Attempting to alter, erase, modify or otherwise compromise, any legitimate software, files, databases or any other form of stored information that is either owned by, been developed by or on behalf of, the Trust or is under the guardianship of the Trust without proper and appropriate authority and/or legitimate intent.
- attempting to copy or move any legitimate software and/or associated material to any storage medium other than that which it is intended by the Trust
- Knowingly causing or facilitating damage to any of the Trust IT systems, resources and/or materials, including any attempt to cause or facilitate negative effect to the reliability of any of the Trust IT application systems, resources and/or materials.
- Preventing, or otherwise hindering, legitimate electronic access by authorised members to either the Trust IT network and application systems, or to any information held within the Trust IT network and application systems.
- corrupting, or knowingly attempting to corrupt, the accuracy and completeness of any information held within the Trust IT network and application systems

Should any users fail to comply with any of these regulations they will be considered to be in breach of the Information Security Policy, and the Computer Misuse Act 1990. This may result in serious disciplinary action being brought against them in line with the Trust disciplinary policy and may lead to the termination of their employment.

6. USER ACCOUNT CONTROL

All users will be given a unique Login to access the Trust network and systems.

Before users can gain access to the Trust IT network (and subsequently any of the Trust computer applications – including email and internet) authorisation MUST be obtained from the Line Manager. Line Managers must complete and submit a New Starter Requirements Form available from the IT ServiceDesk.

When requesting access for a new starter the line manager must ensure that the new user is provided with the minimum access that is required for them to perform their function.

For new users' domain accounts; NHS Mail accounts and folder access requests can only be made via the IT ServiceDesk by named individuals with delegated responsibility (referred to as 'Data Controllers') following approval by the new user's line manager. For access to some folders and information systems the approval by the relevant Information Asset owner will also be required. A minimum of one week's notice is required for the setup of new user accounts. A list of Information Asset Owners and Data Controllers is available from the Trust IG Lead. Queries around information assets should be directed to the Trust Information Governance Lead or Information Governance support.

All relevant changes to an employee's status which require a change to their IT set up or information systems access [e.g. changing a user's folder access or closing a domain account] must be approved by the line manager and where required the Information Asset Owner and request the change via IT ServiceDesk. Examples of relevant changes are role changes, resignation or termination and other interruptions to continuous employment.

To prevent users from inappropriate access to information as they move around the organisation it is important that access rights, especially to sensitive information, are reviewed/revoked when moving to a new area/role with any required changes processed as above. Information access should be the minimum required for the user to perform their function. Access to information must not be retained 'just in case' the user's member transitions back into an area.

On departure from the organisation all users (including secondees, contractors, temporary users and permanent users) will surrender all IT equipment to IT ServiceDesk including but not limited to, computers, iPads, mobile phones, remote VPN access tokens, encrypted USB sticks.

In circumstances where an individual is unavailable for unforeseen reasons, access to their information/documentation held on the Trust equipment may be granted only with the express authorisation of the Chief Information Officer. This includes information on:

- Laptop
- e-Mail
- network drives
- paper information

When a user leaves the organisation the domain account should be closed down immediately, and the user marked as a ‘leaver’ on NHS mail.

Users are not permitted to share their, or others, usernames and passwords to gain access to the Trust network or other information systems.

Users may at their own discretion permit other users to access their e-mail. It is the e-mail owners’ responsibility to ensure that such access is appropriate and does not result in individuals having inappropriate access to sensitive information. Further information in regard to this can be found in Email Policy under delegated authority.

7. SYSTEM SECURITY AND NETWORK USAGE

During initial setup of user accounts, a temporary password may be created. The communication procedures for these temporary passwords shall ensure the security of passwords at all times. Once issued with a temporary password a user MUST change this at first logging into the system.

All users must always operate DBTH equipment using their username and password. Passwords must meet complexity requirements and MUST NOT be shared with anyone. Logging onto the Trust equipment with credentials that users are not authorised to use is not permitted.

All users shall authenticate themselves using a password at the Windows Login. These passwords will as a minimum comply with the following:

- 12 Characters long
- Changed every 365 days

Your Domain Account will lock out (meaning even if the correct password is input, you will not be able to login) if ten incorrect passwords are inputted within a ten-minute time frame.

For further guidance on password security refer to Appendix A.

The Trust staff are responsible for the security of their passwords and accounts and are therefore responsible for all computer transactions that are made with their username and password.

If a password becomes known to another person, it must be changed immediately.

All access to the Trust network must be provisioned only via the IT ServiceDesk

It is mandatory for all users to lock their terminals, workstations, laptops, by pressing ctrl/alt/del (or “windows key” and L), iPads and/or Smartphones when not using their device, even for a short period.

The Trust equipment is configured in order to restrict certain user activities. These restrictions are for support, security, and management purposes. Circumvention of these restrictions without appropriate authorisation may lead to disciplinary action.

Desktop/Laptop software installations must be performed by the Trust IT ServiceDesk. Users are prohibited from installing any software themselves.

All users must not access or attempt to access information to which they do not have a legitimate business need and to which they have not been authorised to view.

It is strictly forbidden for users to knowingly browse, search for or look at any information relating to themselves, their own family, friends, or other persons, without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and of the Data Protection Act.

All data and information residing on the Trust equipment, (e.g. laptops, mobile phones, etc.) that has been allocated to the Trust staff remains the property of the Trust at all times

The illegal copying of copyrighted content onto the Trust equipment is not permitted.

8. DATA STORAGE

Data must be always saved on a network drive.

Staff must seek approval from their Line manager with a valid justification if there is a need to use an external storage such as USB, external hard drive…etc. Request must be submitted via IT ServiceDesk for the authorisation and approval from Head of Digital Operation and Cyber Security

On approved cases, data may be saved to an approved encrypted removal media provided by the IT ServiceDesk. In this event, a copy of all the data must be left on the network as a backup.

All the Trust corporate data should be stored in one of the following locations, and not locally on laptop / desktop hardware:

- Authorised Shared Data Drive
- Home Drive - Referred as H drive
- Microsoft SharePoint sites
- Microsoft Teams channels

Users are not permitted to store personal music or photographs on the Trust network drives.

9. DATA TRANSFER

ANY transfer of Corporate or Patient Identifiable Data outside The Trust boundaries either physically or by electronic means must be approved by the Head of Digital Operations and Cyber Security and the Head of Information Governance PRIOR to any transfer being made.

10. GUEST WI-FI ACCESS

The provision of a 'Guest Wi-Fi' facility at the Trust allows guests and visitors the ability to connect directly to Internet services without compromising the integrity of the Trust network.

The guest network will be monitored on a regular basis to ensure that the service is not abused.

11. INTERNET USAGE

Access to the Internet is provided to support the business, but it may be used for occasional and reasonable personal use e.g. during lunch breaks provided that it does not interfere with the performance of duties and does not conflict with the Trust policies.

Files from the internet, or any images that are displayed must not be downloaded for personal use as there may be any number of issues concerning copyright, viruses, and overall functioning of the computer.

Instant messages and other communications mechanisms made across the internet may not be secure. The Trust authorised communication mechanisms only should be used.

Transactions are not permitted on sites requiring software to be downloaded before proceeding.

The Trust accepts no responsibility for any charges or loss incurred in relation to personal purchases or financial transactions using the Trust IT facilities regardless of cause.

To intentionally access or forward material that is defamatory, pornographic, sexist, racist, online gambling or material whose publication is illegal or risks causing offence or disrepute to the Trust may lead to disciplinary action or prosecution. If access to restricted material is required, a request to the IT ServiceDesk with supporting business justification and Line Manager endorsement should be submitted prior to attempting to access the material / site.

Users must be aware that each website they visit is logged and these logs can be examined to support a disciplinary action.

The Trust prohibits access to websites deemed inappropriate and monitors access and usage. The monitoring information may be used to support disciplinary action.

Sites deemed inappropriate are those with material that is defamatory, pornographic, sexist, racist, on-line gambling, terrorism and/or such sites whose publication is illegal or risks causing offence.

If you have any questions about what is considered to be appropriate or inappropriate use, please check with your manager or the IT Department. Known sites falling within the above categories may be blocked by Trust's web security solution.

Users must not circumvent, cause to circumvent or use tools to circumvent prohibited website controls. If a user inadvertently accesses an inappropriate website, the user must immediately inform their line manager or the IT ServiceDesk.

The use of the Trust IT systems to conduct on-line selling is strictly prohibited.

The internet must not be used for participation in online games.

Messages must not be posted on any internet message board, social networking sites or other similar web-based services that could bring the Trust into disrepute, or which a reasonable person would consider to be offensive or abusive.

12. EMAIL USAGE

DBTH provides NHSmail account to assist employees, third parties, contractors, and temporary staff in the performance of their jobs and its use should be limited to official Trust business.

No employees, third parties, contractors and temporary staff should knowingly use the NHSmail system in any way that may be interpreted as insulting, disruptive or offensive by any other person, or which may be harmful to the Trust. This includes forwarding any received email containing any prohibited material listed below.

Examples of prohibited materials include, but are not limited to:

- sexually explicit messages, images, cartoons, or jokes
- unwelcome propositions, requests for dates, or love letters
- profanity, obscenity, or libel
- ethnic, religious, or racial slurs
- or any other message that could be construed as harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability or religious or political beliefs.

Emails concerning illegal activities must not be sent or forwarded unless they relate to the legitimate business of the Trust. The Head of Information Governance must be notified immediately should any such e-mails be received. These emails must not be forwarded to anyone unless required by IG Lead.

The system may not be used for personal financial gain.

The forwarding of chain letters is strictly forbidden. This includes those purporting to be for charity or other good causes as well as those promising wealth or other personal gain.

Any suspicious emails must be reported following the general reporting procedure. If you are still in doubt, please check the authenticity of these messages by contacting the IT Security Manager, but do not under any circumstances forward these messages to anyone inside or outside of the Trust.

All email messages that are sent externally from the Trust will be passed over networks owned by other people; this is not a secure form of communication. If the content of the message could cause embarrassment or problems for the Trust or cause financial loss, should the contents become known, a more secure method should be used.

The user logged in at a computer will be considered to be the author of any messages sent from that computer. Remember to log-out or lock computers if left unattended (press the “windows” key and the letter “L” key at the same time). Under no circumstances should an e-mail be sent from a PC that is logged in to the network by another person. Email addresses should not be disclosed unnecessarily.

Disclosing email addresses when filling in surveys or other questionnaires will increase the risk of a compromised account or receiving unwanted junk messages.

Email should not be used to send large, attached files (i.e. 15 Megabytes or larger), unless very urgent. Many email systems including those used by the NHS will not accept large files, which are returned and may result in overloading the NHS email system. Egress solution provided by NHSmail should be used to send large amounts of data, whenever possible.

Users should not be open any attachments or click on links contained in the email unless they are expected and from a known sender. Extreme caution should be exercised.

NHS mails must not be automatically forwarded to other non-NHS or Government email addresses e.g. Hotmail, Gmail etc. Refer email and internal communications policy v27 on accessing emails outside the Trust devices.

Users must be aware that the Trust may interrogate email accounts and content (including deleted items) without notice if there appears to be a just cause to do so and information can be used to support disciplinary action

Personal identifiable information, confidential or sensitive information should not be sent via email unless it is encrypted. NHS.net email is automatically encrypted in transit, therefore any email sent from an NHSmail account to another (e.g. xxx@nhs.net toyyy@nhs.net) is secure.

The user sending the email must first confirm the recipients email address, for example verbally over the telephone or through the NHS.net directory.

When sending outside the NHS domain, person identifiable, confidential, or sensitive information must be removed from the email and sent as an encrypted attachment. Any authorised transfer of sensitive information to a non-NHS email should be using encrypted channel. Encryption can be achieved by putting "[Secure]"in the beginning of the subject line of the email.

13. MOBILE DEVICE USAGE

All mobile devices (laptops, tablets, mobile phones) issued by the Trust are intended as a business tool to enable the member of users to perform their role.

Users are prohibited from installing any additional software on the Trust mobile equipment. All software installation for laptops and tablets must only be carried out by the IT ServiceDesk.

Mobile internet and email access via the Trust Mobile devices are subject to the same restrictions as those outlined in sections 9 and 10 above.

Users must ensure that all mobile devices are stored securely at all times and must log off at the end of the working day and ensure that they close down the different systems and applications. Laptops / mobile devices should where possible be kept away from a position where it's contents can be viewed by people not authorised to do so.

Users of mobile computing devices must not allow unauthorised access by third parties including, but not limited to, family and friends.

Passwords relating to mobile devices should never be written down and/or kept with the device.

Mobile devices must be transported securely and may only be left in the boot of a car during the day when there is no alternative method of securing the device. Devices must not be left in any vehicle overnight.

The antivirus software must be kept up to date by regular connection (at least every 30 days)

All Mobile computing devices (tablets and laptops) are encrypted. In order to ensure synchronisation all devices must be connected to the secure Trust network at least every 30 days.

Peripheral device of any kind (e.g. digital cameras, PDAs, USB pen drives, etc.) shall not be connected on any of the Trust computers. Circumstances where the exceptions are made based on the business justification and the approval from the Head of Digital and Cyber Security.

Under no circumstances should personnel identifiable data be copied to the C: drive on a laptop or tablet device.

If a mobile device is lost or stolen, then it should be immediately reported to the line manager, IT ServiceDesk and also the incident should be reported via the Datix.

Employees and users of the Trust systems and equipment are not permitted to take their IT equipment / devices and use them outside of the UK unless they have been granted appropriate permission from the Head of Digital Operations and Cyber Security.

14. ADDITIONAL RESPONSIBILITIES FOR LINE MANAGERS

All Line Managers have a duty to meet the obligations as users but in addition, they have additional responsibilities as line managers of the Trust users (including contractors). These include:

- Ensure users maintain adequate protection of their systems and equipment at all times particularly when left unattended.
- Ensure all staff have a copy of this policy.
- Ensure that all temporary, agency and contracted staff have time-limited access to systems based on their role
- Users' access is revoked, and equipment returned when users move departments / leave the organisation.

15. REMOTE ACCESS

Who can access The Trust Remotely; The Trust supports the remote access to it's information systems by providing a remote access service to enable authorised users to connect remotely to the Trust network when they are not at the Trust office location.

Any Third Party that has signed a contract with the Trust to provide support, maintenance, or services.

Any Third Party that requires remote access to services or equipment in order to meet contractual requirements of provided services.

What can be accessed; Remote access will only be granted to servers / equipment that has been previously agreed at the approval stage. Third Party access to the Trust information systems are limited only via the approved VDI remote access mechanism.

All the remote endpoints that connect to the VDI endpoints must comply with the minimum OPSWAT compliance standard defined by the Trust. Devices that do not meet this baseline will be denied access to the VDI environment.

Where possible, access to other devices, outside the original approval, will be restricted. Whilst every reasonable effort is made to restrict access to other devices, it may not always be practice. In these circumstances Third Parties are expected to limit their access to originally agreed servers / equipment and not attempt access to others.

When working from home users should ensure that they have the appropriate facilities to support Remote Access to the Trust network i.e. their own uninterrupted broadband connection.

What cannot be accessed; Third Parties are forbidden access to any servers / equipment / systems that have not been originally agreed at the approval stage.

16. MICROSOFT TEAMS

To allow individuals to work in a more accessible way, Microsoft Teams has been permitted as an appropriate application for staff across the NHS to use. The Microsoft Teams application has been installed on user's laptops and this acts as a way for meetings to held virtually as well as messages and files shared across different directorates and NHS staff. Although Microsoft Teams has been approved as an appropriate system to use, staff should continue to follow the necessary supporting policies and procedures (IMT Security, Acceptable Use of IT, Confidentiality and Code of Conduct etc) to ensure no breaches and that the policies are followed appropriately.

17. PROCEDURE FOR INVESTIGATION OF SUSPECTED POLICY BREACHES

Suspected misuse of the Trust's internet or NHSmail systems may be identified (but not exclusively) by:

- Routine monitoring.
- Eyewitness accounts.
- Personal experience.
- Actual evidence (e.g. examples of inappropriate Emails).
- Evidence of poor performance or time-wasting.
- External complaints or queries received.

The relevant line manager should initially discuss the suspected abuse with the Information Governance department to determine what action should be taken and where required an investigation will be carried out in accordance with the Trust's Disciplinary Procedure.

Suspicions or allegations of fraud and/or corruption in connection with the use of the internet and/or NHSmail system must be referred immediately to the Trust's Local Counter Fraud Specialist (LCFS). Where there is any doubt as to whether an allegation or suspicion relates to fraud and/or corruption, the LCFS must be contacted for advice.

No discussions should be entered into with the suspected individual by their Line Manager or any other member of staff without agreement and guidance from the LCFS or the Head of Information Governance.

Where a suspicion or allegation involves any other illegal activity (except fraud), the Trust will consider referring the matter to the Police and isolate any IT equipment for appropriate forensic analysis as outlined in the IMT Security Policy (CORP/ICT 2).

18. MONITORING

Monitoring of Compliance; Random audits will be conducted by the IT Department for core systems and individual System Managers for separate departmental systems.

Accounts with no activity for more than three months will be disabled.

In line with current NHS Guidelines, accounts with no activity for more than six months will be archived unless specific approval has been sought in advance. After twelve months they will be deleted.

If there is evidence that a Third Party is not adhering to the guidelines set out in this policy, the Trust reserves the right to examine PC usage/content and to take disciplinary action, which may lead to the termination of contract.

Third Parties should be aware that the Trust has the right to monitor accounts / account usage.

At all times, the Trust reserves the right to monitor all accesses, transfers and communications.

Third Parties should have no expectation of privacy whilst connected to Trust systems.

Monitoring of document Compliance; Compliance with the policies and procedures laid down in this document will be monitored via the Information Governance Lead, together with IT Security Manager, Head of Digital Operations and Cyber security, independent reviews by both Internal and External Audit on a periodic basis.

The Trust IG Lead is responsible for the monitoring, revision and updating of this document.

This policy will be reviewed 3 yearly, and in accordance with the following as required:

- legislative changes
- good practice guidance
- case law
- significant incidents reported
- new vulnerabilities
- organisational changes

19. EQUALITY IMPACT ASSESSMENT

An Equality Impact Assessment (EIA) has been conducted on this procedural document in line with the principles of the Equality Analysis Policy (CORP/EMP 27) and the Fair Treatment for All Policy (CORP/EMP 4).

The purpose of the EIA is to minimise and if possible remove any disproportionate impact on employees on the grounds of race, sex, disability, age, sexual orientation or religious belief. No detriment was identified.

20. ASSOCIATED TRUST PROCEDURAL DOCUMENTS

Equality Analysis Policy - CORP/EMP 27
Fair Treatment for All Policy – CORP/EMP 4
Freedom to Speak Up Policy 'Speak up to make a difference' – CORP/EMP 14
Fraud, Bribery and Corruption Policy and Response Plan – CORP/FIN 1 (D)
IMT Security Policy – CORP/ICT 2

21. REFERENCES

All staff members are required to comply in particular with the provision of the following legislation and Department of Health guidance:

- Data Protection Act 2018
- General Data protection Regulation (UK GDPR) 2021
- Computer Misuse Act 1990
- Fraud Act 2006
- Copyrights, Designs & Patents Act 1990
- Human Rights Act 1998
- Freedom of Information Act 2000
- Access to Health Records Act 1990
- The Health & Social Care Act 2012
- NHS Digital : Records Management - Code of Practice 2016
- Mental Health Capacity Act 2005
- NHS Confidentiality Code of Practice 2003
- IT Acceptable Use Policy CORP/ICT 29

22. APPENDIX A

Poor and weak passwords have the following characteristics:

- The password contains less than twelve characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like “aaabbb”, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Following are a few guidance points for **creating a strong password**

- Avoid using predictable passwords (such as dates, family, fantasy characters, favourite sports team and pet names).
- Avoid the most common passwords that criminals can easily guess (like 'passw0rd').
- Avoid using the same password across your personnel and Trust accounts. If one of your passwords is stolen, you don’t want the criminal to also get access to other accounts.

A good way to create a strong and memorable password that’s also hard for someone else to guess is to use a passphrase combining three random words. Numbers and symbols can still be used if needed, for example: ‘3redhousemonkeys27’

- Passwords must never be written down or stored online.

Here is a list of password ‘don'ts’:

- Don't reveal a password to anyone.
- Don't reveal a password in an email message.
- Don't talk about a password in front of others.
- Don't hint at the format of a password (e.g., "my family name").
- Don't reveal a password on questionnaires or security forms.
- Don't share a password with family members.
- Don't reveal a password to co-workers while on leave.

What to do if your password is stolen?

An account or password is suspected to have been compromised, report the incident immediately to the Trust IT ServiceDesk and change all passwords.

APPENDIX B – EQUALITY IMPACT ASSESSMENT PART 1 INITIAL SCREENING

Service/Function/Policy/Project/ Strategy	Care Group/Executive Directorate and Department	Assessor (s)	New or Existing Service or Policy?	Date of Assessment
APDs – Development & Management Process	*Director of Nursing, Midwifery & Quality*	*Richard Dickinson*	*Existing Policy*	*September2016*

1) Who is responsible for this policy? Name of Care Group/Directorate: *Directorate of Nursing, Midwifery & Quality*

2) Describe the purpose of the service/function/policy/project/strategy? Who is it intended to benefit? What are the intended outcomes? *To support the authors in the development and review of APDs and create a unified process*

3) Are there any associated objectives? Legislation, targets national expectation, standards: *Trust standard*

4) What factors contribute or detract from achieving intended outcomes? – noncompliance within services

5) Does the policy have an impact in terms of age, race, disability, gender, gender reassignment, sexual orientation, marriage/civil partnership, maternity/pregnancy and religion/belief? Details: [see Equality Impact Assessment Guidance] - *No*

□ **If yes, please describe current or planned activities to address the impact** [e.g. Monitoring, consultation] –

6) Is there any scope for new measures which would promote equality? [any actions to be taken] *No*

7) Are any of the following groups adversely affected by the policy? No

Protected Characteristics	Affected?	Impact
a) Age	*No*	
b) Disability	*No*	
c) Gender	*No*	
d) Gender Reassignment	*No*	
e) Marriage/Civil Partnership	*No*	
f) Maternity/Pregnancy	*No*	
g) Race	*No*	
h) Religion/Belief	*No*	
i) Sexual Orientation	*No*	

8) Provide the Equality Rating of the service / function /policy / project / strategy – tick (✓) outcome box

Outcome 1 ✓	**Outcome 2**	**Outcome 3**	**Outcome 4**

If you have rated the policy as having an outcome of 2, 3 or 4, it is necessary to carry out a detailed assessment and complete a* **Detailed Equality Analysis form – see CORP/EMP 27

Date for next review: ***January 2020***

Checked by: ***Richard Dickinson*** **Date: 22 January 2017**