West Hertfordshire Teaching Hospitals NHS Trust

ICT Acceptable Use Policy

Controlled document

This document is uncontrolled when downloaded or printed

Reference number	WHHT: IT023
Document type	Policy
Version	3
Author's name & job title	Luke Drewer, Cyber Security Lead
Department/Speciality	ICT Information Security
Division	Corporate
Reviewed by	Informatics Group
Review date	November 2023
Approved by PGRG	20th February 2024
Next review date	30th November 2026
Target audience	All WHHT Staff
Search terms	'Information Governance', 'Information Security', 'Acceptable Use', 'Internet Use', 'Email Use'
Previous document name (if different)	Internet Acceptable Use Policy, Email Acceptable Use Policy, IT Code of Conduct

Dissemination: By default, **all** controlled documents are uploaded to the document library on the intranet, unless explicitly asked otherwise. **If necessary**, please use the box below to highlight where else the document should be published.	
Publish on Trust Intranet:	**http://wghintra01/environment/security/policies.asp**

Contribution List

Key individuals involved in developing this version of the document

Name	Designation
Jo Brown	Head of Technical Design & Assurance
Luke Drewer	Cyber Security Lead

Peer Reviewed By

Name	Department
Nicola Bateman	Information Governance
Caroline Lankshear	HR
Kate Ewer	Communications
Richard Burridge	Chief Clinical information Officer (CCIO)
Victoria Houghton	Head of EPR Adoption & Optimisation
John Medany	Senior Enterprise Infrastructure Architect

Change of History

Version	Date	Author	Reason for change
0.1	Jan 2019	Aleksandra Lukaszewicz	**e.g.** New Policy to combine and replace existing policies
1.0	Oct 2020	Jo Brown	To replace existing policies: Internet Acceptable Use Policy, Email Acceptable Use Policy, IT Code of Conduct
2.0	Oct 2021	Jo Brown	Added two new sections for 'Use of Strong Passwords' and 'Storage of Information Electronically'
3.0	Oct 2023	Luke Drewer	Amended objectives to reflected changes Amended 6.2Guidelines for IT Equipment Use Updated broken links Revised Social Media Section Added section 'WhatsApp and other Instant Messaging Apps' Updated policy template

Abbreviations and Acronyms

Abbreviations and Acronyms	Description
DPA	Data Protection Act
GDPR	General Data Protection Regulations
ICT	Information and Communications Technology
MDT	Multidisciplinary Team
PGRG	Policy & Guideline Review Group
QSG	Quality & Safety Group

Contents

1. Introduction 5
2. Objectives 5
3. Definitions 5
4. Scope 5
5. Responsibilities 6
5.1 All Staff 6
5.2 Senior Information Risk Owner 6
5.3 Information Governance Manager 6
5.4 Cyber Security Lead 6
6. Conditions of Acceptable Use 6
6.1 Use of Information Systems 6
6.2 Guidelines for IT Equipment Use 7
6.3 Internet Acceptable Use 9
6.4 Email Acceptable Use 10
6.5 Social Media Use 10
6.6 WhatsApp and other Instant Messaging Apps 11
6.7 Storage of Information Electronically 12
7. Monitoring & Compliance 15
8. Safeguarding 16
9. Patient & Carer Involvement 16
10. References 16
11. Related Policies and Guidelines 16
12. Equality Impact Statement (EIA) 17
Appendix 1 – Equality Impact Assessment ..... **Error! Bookmark not defined.**
Appendix 2 - Legal Requirements ..... **Error! Bookmark not defined.**

1. Introduction

The policy explains how the Trust's ICT facilities should be used. It is your responsibility to ensure you understand and comply with this policy. It ensures that:

- You understand your responsibilities and what constitutes abuse of the ICT facilities.
- Computers and personal data are not put at risk.

The ICT Acceptable Use Policy is one of a number of policy documents that link to the Trust's Information Security Policy and ensures there is an adequate Information Governance Management Framework (as per the Data Security and Protection Toolkit), to support the current and evolving Information Governance and Cyber Security agenda. It also meets the current legal requirements defined in appendix 2, Legal Requirements.

2. Objectives

The aim of this policy is to ensure that the Trust's ICT facilities are used: safely, lawfully and equitably. This ICT Acceptable Use Policy is intended to provide a framework for such use of the Trust's IT resources.

The policy covers the following areas for acceptable use:

- Responsibilities and use of ICT assets
- Use of e-mail, Internet and social media
- Use of WhatsApp and other Instant Messaging Apps
- Use of removable media
- Network usage (Including passwords/user access control)
- Storage of information electronically

The policy should be interpreted such that it has the widest application and so as to include new and developing technologies and uses, which may not be explicitly referred to.

3. Definitions

Term	***Meaning/Application***
SHALL	*This term is used to state a **Mandatory** requirement of this policy*
SHOULD	*This term is used to state a **Recommended** requirement of this policy*
MAY	*This term is used to state an **Optional** requirement*

4. Scope

This policy applies to the use of ICT facilities including information, data, electronic and computing devices, telephony and network resources to conduct the Trust business or interact with internal networks and business systems, whether owned or leased by the Trust, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at the Trust are responsible for exercising good judgment regarding appropriate use ICT facilities in accordance with the Trust policies and standards, and local laws and regulation.

This policy applies to all uses of ICT facilities i.e. employees, contractors, consultants, agency, bank, locum and other workers at the Trust, including all personnel affiliated with third parties and partner organisations.

This policy applies to all equipment that is owned or leased or rented by the Trust.

5. Responsibilities

5.1 All Staff

It is the responsibility of all staff to abide by this policy.

5.2 Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) is accountable for information risk within the Trust and advises the Board on the effectiveness of information risk management across the organisation. This includes establishing the Board's appetite for Information Risk, and communicating information security policies throughout the Trust. Operational responsibility for Information Security shall be delegated by the SIRO to the Trust's Information Security Manager.

The role of SIRO is undertaken by the Trust Chief Information Officer.

5.3 Information Governance Manager

The Information Governance Manager and is responsible for managing the Information Governance agenda across the Trust. This will include monitoring compliance with the GDPR and DPA processes.

5.4 Cyber Security Lead

The Cyber Security Lead is responsibility for managing the Cyber Security Agenda across the Trust and for reviewing and assurance of security measures in place for existing and new information assets.

6. Conditions of Acceptable Use

6.1 Use of Information Systems

a) Use Strong Passwords

- Choosing a strong password is essential. When we say a password is 'strong', we mean it's hard to guess.
- **Avoid the really obvious choices** - Lots of people really do choose things like '12345678', 'qwerty123' or 'password123'. Or they use the day of the week and date they changed their password on. Users shall not use obvious weak passwords and will adopt strong passwords.
- In order to have a strong password that's still memorable, try using three random words - like 'winter warming heart'. It provides a good compromise between protection and usability. If you can think of a little story or mental picture to link the words, that can help the password stick in your mind. If you want some extra strength you can, add capitals, numbers and special characters. But avoid obvious patterns, like capitalising the first letter of a word.

b) Unauthorised Information Access

- An individual user shall only be authorised to access information relevant to their work.

- Accessing or attempting to gain access to unauthorised information shall be deemed a disciplinary offence.
- When access to information is authorised, the individual user shall ensure the confidentiality and integrity of the information is upheld, and to observe adequate protection of the information according to NHS policies as well as legal and statutory requirements. This includes the protection of information against access by unauthorised persons.
- Users shall not attempt to circumvent any security controls in place to protect Trust systems, information and/or data.

c) Misuse of Information Systems

- Use of NHS information systems for malicious purposes shall be deemed a disciplinary offence. This includes but is not limited to:
  - Penetration attempts (“hacking” or “cracking”) of external or internal systems.
  - Unauthorised electronic eavesdropping on or surveillance of internal or external network traffic or user activity.
  - Discriminatory (on the grounds age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage and civil partnership and pregnancy and maternity), or derogatory remarks or material on computer or communications media; this includes but is not limited to sending offending material as embedded or attached information in e-mails or other electronic communication systems.
  - Acquisition or proliferation of pornographic or material identified as offensive or criminal.
  - Deliberate copyright or intellectual property rights violations, including use of obviously copyright-violated software.
  - Storage or transmission of large data volumes (over 250Mb) for personal use, e.g. personal digital images, music or video files or large bulk downloads or uploads.
- Users accessing or attempting to access medical or confidential information concerning themselves, family, friends or any other person without a legitimate purpose and prior authorisation from senior management is in breach of the DPA, strictly forbidden and shall be deemed a disciplinary offence.
- Use of NHS information systems or data contained therein for personal gain, to obtain personal advantage or for profit is not permitted and shall be deemed a disciplinary offence.
- If identified misuse is considered a criminal offence, criminal activity shall be filed with local police and all information regarding the criminal actions handed over to the relevant authorities.

6.2 Guidelines for IT Equipment Use

a) Physical Protection

- Users shall not eat or drink in the vicinity of any ICT equipment.

- Users shall not expose any ICT equipment to magnetic fields that may compromise or prevent normal operation.
- Users shall not knowingly expose any ICT equipment to external stress, sudden impacts, excessive force or humidity.
- Only authorised ICT support personnel shall be allowed to open NHS IT equipment and equipment cabinets.
- If left unattended in semi-controlled areas such as conference centres or customer offices, laptops should be locked to a fixed point using a physical lock available from ICT Service Portal.
- Portable equipment shall never be left unattended in airport lounges, hotel lobbies, trains and similar areas as these areas are insecure.
- Portable equipment shall be physically locked down or locked away when left in the office overnight.
- Portable equipment shall never be left in parked cars, unless completely invisible from outside the vehicle and protected from extreme temperatures.
- Portable equipment shall not be checked in as hold luggage when travelling, but treated as hand or cabin luggage at all times.

b) General Use

- All systems and devices provided by the Trust are subject to the same conditions of use whether they are used remotely (including home) or on a Trust site.
- When a Trust owned ICT device is no longer required, the item shall be returned to the ICT department for appropriate redeployment or disposal.
- Only the ICT department are authorised to move ICT equipment. Unauthorised movement of ICT equipment may have an adverse impact on the delivery of patient care or the running of essential services, therefore, you shall not move ICT equipment (refer to the Management of ICT Equipment policy).
- Faulty/broken ICT equipment shall be reported to the ICT Service Desk at the earliest opportunity. Where ICT equipment cannot safely be used it should be withdrawn from use and labelled clearly “FAULTY DO NOT USE”.
- All ICT equipment must be disposed of by the ICT department and in accordance with the Trust Waste Management policy.
- Use of the Trust’s ICT systems and equipment is primarily for the purpose of your job role within the Trust and as such, users of Trust systems should not have any expectations as to the privacy of their activities whilst using them e.g. personal documents, images and files can be viewed by authorised IT personnel.
- All network connections must be authorised and installed by the ICT department. Do not connect any device (desktop, laptop, printer, router, modem, wireless network, etc.) to the Trust Network or any part of the Trust system unless the device is owned by the Trust or the connection has been approved and set up by the ICT department.

- Any device, software or web based service detected on the Trust's Network that has not been authorised and installed by the ICT department shall without warning, be removed or disabled.
- All software shall have an appropriate license provide to ICT before any approval for installation and use shall be granted.
- Users shall return any ICT equipment (mobile phones, laptops, tablets, etc.) assigned to them, to their line manager before leaving the Trust or transferring to a new role within the Trust.
- Users shall lock their desktop/terminal/workstation/laptop/mobile device (using the Windows+L function or other applicable method) when left unattended, even for a short period.
- User shall never reveal their account passwords to others or allow them to be used by others. This includes family and other household members when work is being done at home.
- Any ICT equipment or software received from outside parties must be evaluated and approved by the ICT department prior to use in the Trust. Staff shall check with ICT before agreeing to accept any ICT equipment not supplied by the Trust's ICT department.
- Only authorised ICT personnel shall be allowed to reconfigure or change system settings on ICT equipment.
- Users shall not download or copy any material onto the Trust ICT equipment that may violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Trust.
- Users shall not use privately owned storage devices or storage devices owned by third parties for transfers of NHS data.
- The lost or theft of any device shall be immediately reported to the 24/7 ICT Service Desk and raised as a Datix incident. If the device is stolen, the user shall also report this to the police and obtain an incident number, which must be included on the Datix incident.
- Laptops shall be connected to the Trust network at least once every 2-weeks to ensure essential security and virus protection updates can be applied. Failure to do so may result in laptops being removed from being able to connect to the Trust network.

6.3 Internet Acceptable Use

- Information found on the Internet is subject to minimal regulation and as such must be treated as being of questionable quality. You should not base any business-critical decisions on information from the Internet that has not been independently verified.
- Internet access via the NHS infrastructure is primarily provided for business purposes. For the purpose of simplifying everyday tasks, limited private use may be accepted. Such use includes access to web banking, public web services and phone web directories.

- Excessive personal use of the Internet during working hours shall not be tolerated and may lead to disciplinary action.
- Users shall not use Internet-based file sharing applications, unless explicitly approved and provided as a service.
- Users shall not upload and download private data (e.g. private pictures) to and from the Internet.
- Users shall not download copyrighted material such as software, text, images, music and video from the Internet.
- Users shall not use NHS systems or Internet access for personal advantages such as business financial transactions or private business activities.
- Users shall not use their Trust's identity (i.e. using your Trust e-mail address) for private purposes such as on social media, discussion forums.
- Users shall not use the Trust guest Wi-Fi to access any confidential information or patient records without additional security arrangements.

6.4 Email Acceptable Use

- The Trust uses the NHSmail system. It is your responsibility to ensure you understand and comply with the NHSmail Acceptable Use policy (https://portal.nhs.net/Home/AcceptablePolicy), which ensures that:
  - You understand your responsibilities and what constitutes abuse of the NHSmail service.
  - Computers and personal data are not put at risk.
  - You understand how NHSmail complies with the General Data Protection Regulation (GDPR)
- Every email is considered public record and therefore, discoverable under the Freedom of Information Act 2000 – never attempt to delete, modify, or hide any email communication to avoid disclosure.
- It is essential that emails containing patient related information are not stored in your email inbox but transferred as soon as practicable to the patient record.
- Users shall include the Trust standard signature in their emails.
- Users should use the Trust email Online archive for retrieval of old emails rather than their mailbox to avoid their mailbox filling up.
- Users shall secure their NHSmail account with provided and supported Multi Factor Authentication.

6.5 Social Media Use

- Employees are personally responsible for the content they publish on blogs, wikis, or any other form of user-generated media. When online, you should use the same principles and standards that you would apply to communicating in any other media with people you do not know.
- You should identify yourself by giving your name and, when relevant, role at WHTH if you are discussing WHTH or NHS related matters. You must make it clear you are speaking for yourself and not on behalf of WHTH or NHS.

- You shall not breach data protection laws or patient confidentiality.
- You shall not publish images or text that might be considered as harassment or are discriminatory, offensive, inflammatory, or abusive which constitute an invasion of privacy, or cause annoyance, inconvenience, or needless anxiety or which promote violence. This includes the promotion of discrimination based on factors such as age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage and civil partnership and pregnancy and maternity.
- Do shall not make, post or share slanderous, defamatory, false, obscene, indecent, lewd, pornographic, violent, abusive, insulting, threatening or harassing comments or images.
- Be aware that people who join your networks and participate in groups that you are a member of may be colleagues, clients, journalists, or suppliers. It may also be possible that people may not be who they say they are, and you should bear this in mind when participating in online activities.
- If you publish content to any website outside of WHTH that could be perceived to have a connection to the work you do or subjects associated with WHTH, you shall display a disclaimer such as:

  "My postings on this site reflect my personal views and don't necessarily represent the positions, strategies or opinions of WHTH"
- You shall not use social media in any way to attack or abuse colleagues.
- You shall not post any material that infringes any copyright, database right or trademark of any other person or organisation including posting copyrighted information in a way that violates the copyright of that information.
- You shall not provide WHTH or others confidential information or other propriety information on external websites. Do not publish or report on conversations that are private or internal to WHTH.
- If you are contacted by the media via social media platforms you will need to talk to the Communications Team (westherts.communications@nhs.net).
- You should not use social media to "whistleblow" without already having raised concerns through the proper channels. All staff should be aware that the Public Interest Disclosure Act 1988 gives legal protection to employees who wish to whistleblow any concerns.

6.6 WhatsApp and other Instant Messaging (IM) Apps

Messaging apps have different levels of encryption. Messages are generally encrypted through transmission but are unencrypted once they are received. This means that anybody can access the messages and their contents if they can access the phone.
The ongoing link and data sharing between WhatsApp and its owner, Facebook, is unclear and should their policy change in the future, patients' confidentiality may be at risk.
Messages sent via these unapproved IM apps may be stored on servers located in the US, which has laws that permit several government agencies to access the information if they so wish. The US is also outside of the permitted geography for NHS information to be

stored and processed, which also puts the Trust at risk of the breaching the UK General Data Protection Regulation.

- The instant messaging app that is approved by the Trust is Microsoft Teams, logged in with your NHS account. This is because NHS Teams can only be accessed by authorised users. It is possible to accidently add a random user or contact from outside the organisation on most other IM applications. Teams is available on any internet connected devices, including personal devices.

- Instant Messaging apps such as but not limited to WhatsApp, Facebook Messenger and Snapchat have not been approved by the Trust and should not be used.

- You shall not use WhatsApp or other IM apps to share patient or other sensitive information in any format and is a breach of this policy and should be reported as an Information Governance Incident on Datix.

6.7 Storage of Information Electronically

- The Trust provides each user with storage space for data. You are likely to have access to a minimum of four storage areas or drives, a local computer drive (the 'C' drive), two network drives ('G' department shared and 'H' user home drives) and a SharePoint area within NHS.NET. Patient Identifiable Data (PID) must not be stored in such areas. PID must be stored in the most appropriate clinical system stores only, such as EPR.
- Think about what and where you are saving your information and how long you are keeping for. It is your responsibility to ensure it is saved in the right place, is reviewed regularly and only stored for as long as is required in line with Trust policies and procedures governing records management, retention & disposal.
  - Local Computer Drives
- A local computer drive, such as the 'C' drive, is located on the computer itself. When a user logs on to the computer, they are given a default (automatic) access to a folder on the 'C' drive called "My Documents" where information can be saved.
- Local computer drives are not 'backed-up' centrally by the ICT department. Any information saved on them, and therefore is at risk of being lost should the computer be stolen or a fault develops on the computer. The ICT department may attempt to rescue locally stored information but this cannot and will not be guaranteed. Any information saved on a local computer drive is done so at the users own risk.
- Under no circumstances should Trust business or clinical information be saved on a local computer drive.
  - Network Computer Drives
- A network computer drive, such as department and user home drives, is located on one of the Trust servers. It is each Users responsibility to ensure all information stored on a network computer drive is saved in a structured manner that complies with Trust policies and procedures governing records management, retention & disposal.

- All information stored on a network computer drive is subject to search and disclosure under the Freedom of Information Act.
- Under no circumstance should personal or private information be stored on a network computer drive. Any non-work-related information found on a network drive can be removed without discussion.
- **Under no circumstances should large media[1] files or large numbers of media files be stored on shared drive.** If you have a requirement for storing large media files or large numbers of media file types please contact the ICT department to discuss the best way of doing this.

  - Users Home Drive (sometimes referred to as H-drive)

- A Users home drive is allocated to an individual user as a secure storage area for saving work-related items that are personal, such as email PST files. It must not be used to store information that may need to be shared with or accessed by other colleagues.
- No other user will be granted right of access to an individuals' home drive, except where that individual is on a prolonged period of unexpected absence. Request for such access must be requested through the ICT Service Portal for appropriate approval.

  - Department Shared Drives (sometimes referred to as G-Drive)

- A department will have one or more share drives. These are collaborative areas for storing data that needs to be shared between two or more users. **The majority of Trust information should be stored on the G-drive.**
- Users are responsible for making work-related files available for use during periods of planned absence or holiday. These should be held on the appropriate department drive as part of the normal collaborative working arrangements so they can be readily accessed.

  - SharePoint on NHS.NET

- Any User with a Trust NHSmail account also benefits from having a small amount of storage in the NHSmail O365 Shared Tenant service. This service enhances the existing NHSmail platform by enabling staff in health and social care to work more efficiently and collaboratively, through more readily and securely shared information between health and social care organisations.
- It is your responsibility to ensure you understand and comply with the NHSmail Acceptable Use policy (https://portal.nhs.net/Home/AcceptablePolicy), when using NHSmail O365 Shared Tenant service.

  - User Profiles

- The Trust provides each user with a 'Roaming User Profile'. It contains information specific to a user and is the thing that ensures no matter which computer you log onto in the Trust, your personal settings such as desktop items (including files and shortcuts), Internet cookies, printer connections, application settings (such as Outlook Email settings) and network computer drives always travel with you.

[1] 'Media files' refers to any Images, Video or Audio files.

- The bigger your profile, the longer it may take for you to log on to a computer – therefore, do not store yours files or folders on your computer ‘Desktop’

  - Staff Leaving the Trust

- Before leaving the Trust or if network access is no longer required, it is the responsibility of the user and their Line Manager, to transfer any work-related information held on local and network drives to appropriate alternative folders according to the storage arrangements for their department.
- Any information held on the H-drive will be deleted by the ICT department once a user has left the Trust.

7. Monitoring & Compliance

1	Following local and national policies and guidelines, what key elements require monitoring?	List elements to be monitored	a. % of staff successfully completing the Level 1 Data Security Awareness Training b. No of findings from Penetration testing c. No of information security events reported to the ICT Service Desk
2	Who will lead/be accountable for monitoring?	Lead title and/or MDT	a. % of staff successfully completing the Level 1 Data Security Awareness Training (**Information Governance Manager**) b. No of findings from Penetration testing (**Information Security Manager**) c. No of information security events reported to the ICT Service Desk (**Information Security Manager**)
3	Describe how the key elements will be monitored?	List tools to evidence compliance	a. % of staff successfully completing the Level 1 Data Security Awareness Training (**Training system**) b. No of findings from Penetration testing (**Pen test report**) c. No of information security events reported to the ICT Service Desk (**ITSM**)
4	How frequently will each element be monitored?	List frequency of monitoring for each element	a. % of staff successfully completing the Level 1 Data Security Awareness Training (**annually**) b. No of findings from Penetration testing (**annually**) c. No of information security events reported to the ICT Service Desk (**monthly**)
5	Explain the protocols for escalation in the event of problems?	List the processes of escalation	a. Security Panel b. Trust Leadership
6	Which Committee/ Panel/ Group will reports go to?	List the Committee/Panel/ Group/Peer Review that the reports will go to	a. Security Panel

7	Explain how the policy/guideline will be disseminated within the Trust?	List ways identifying how this document will be shared and how it will be recorded that appropriate staff have been made aware of the document and where to find it	a. Notification of a new/revised policy and copies of it shall be made available to personnel via the Trust Intranet (http://wghintra01/imt/security.htm) and communicated through e-update.

8. Safeguarding

Not applicable

9. Patient & Carer Involvement

Not applicable

10. References

1. NHS Digital. NHSmail Acceptable Use policy. Available: https://portal.nhs.net/Home/AcceptablePolicy. Last accessed May 2020.
2. UK Government (April 2020). Cyber Essential. Available: https://www.gov.uk/government/publications/cyber-essentials-scheme-overview. Last accessed May 2020.

11. Related Policies and Guidelines

- Information Security Policy
- Management of ICT Equipment Policy
- Waste Management policy

12. Equality Impact Statement (EIA)

What is an equality impact assessment?

There are many benefits in conducting an equality impact assessment (EIA) prior to making business decisions about policies, clinical guidelines or any other work that may potentially impact on a wide range of people with protected characteristics. Equality impact assessments should not be seen as an afterthought once decisions have already been made.

Benefits:

- Improved capacity to consider equality, diversity and inclusion as part of business management
- Reduced costs as a result of not having to revisit a policy/project
- Take into account a diverse range of views and needs
- Enhanced reputation as a Trust that is seen to understand and respond positively and proactively to diversity.

Whatever approach you take to an equality impact assessment, case law has established that you should keep an accurate, dated, written record of the steps you have taken to analyse the impact on equality. This will help you to check whether you are complying with the duty and it will be useful if your decisions are challenged.

When completing an equality impact assessment you should consider:

- Treating a person worse than someone else because of a protected characteristic (known as direct discrimination)
- Putting in place a rule or way of doing things that has a worse impact on someone with a protected characteristic than someone without one, when this cannot be objectively justified (known as indirect discrimination)
- Treating a disabled person unfavourably because of something connected with their disability when this cannot be justified (known as discrimination arising from disability)
- Failing to make reasonable adjustments for disabled people.

Equality impact assessment process

Stage 1 (Screening)

This stage provides an opportunity to explore whether the policy decision may have a negative, neutral or positive impact on different groups of people.

- If yes, use the ‘comments’ column to describe what this impact could be.

- If no, outline how have you arrived at this conclusion.

- If unsure use the ‘comments’ column to describe what you need to do to find out.

Stage 2 (Full Assessment)

This should be carried out in compliance with policy HR028 Equality & Human Rights Policy.

Does this policy/guideline affect one group less or more favourably than another on the basis of:				
				Comments
1	Age (younger people & children& older people)		no	
2	Gender (men & women)		no	
3	Race (include gypsies and travellers)		no	
4	Disability (LD, hearing/visual impairment, physical disability, mental illness)		no	
5	Religion/Belief		no	
6	Sexual Orientation (Gay, Lesbian, Bisexual)		no	
7	Gender Re-assignment		no	
8	Marriage & Civil Partnership		no	
9	Pregnancy & Maternity		no	
	Is there any evidence that some groups maybe affected differently?		no	
	Could this document have an impact on other groups not covered by a protected characteristic? (e.g.: low wage earners or carers)		no	
	If '**NO IMPACT'** is identified for any of the above protected characteristics then no further action is required.			
	If '**YES IMPACT**' is identified a full impact assessment should be carried out in compliance with HR028 Equality & Human Rights Policy and linked to this document			

Any other comments:
Please use this box to add any additional comments relevant to the assessment

Assessment completed by:	*Luke Drewer, Cyber Security Lead*	Date completed:	November 2023

If you have any queries or concerns about completing the EIA form, contact the Trust's Inclusion & Diversity Team at WestHerts.Inclusion@nhs.net