Public – To be published on the Trust external website

IT & Telephony Procurement, Re-assignment and Disposal Policy

Ref: IT-0020-v8

Status: Ratified
Document type: Policy

Contents

1 Introduction

Asset Management in one form or another is fundamental to cyber security. Organisations need to have policies and procedures in place to purchase, manage and dispose of IT assets. This is recognised by the National Cyber Security Centre, and sequences of the Data Security and Protection Toolkit require Trusts to have policies in place to control and monitor assets.

This Policy supports these requirements by ensuring the security and integrity of the Trust's IT infrastructure.

Any IT & Telephony equipment used for Trust purposes, this includes laptops, smartphones and chargeable software, must be officially purchased and tested for compatibility. Only IT & Telephony equipment purchased in accordance with this policy must be connected to the Trust IT systems. Non-standard equipment requests must be discussed with the **Digital and Data Services** and assessed to ensure that items meet the necessary standards to allow them to be purchased.

This policy supports Our Journey To Change specifically in terms of our second goal 'To co create a great experience for our colleagues' by helping to ensure that our colleagues have a workplace that is fit for purpose.

We do this by:

- Ensuring colleagues have the necessary IT tools to carry out their roles
- Supporting individually any workplace adjustments that might be needed

It also supports us delivering third goal 'To be a great partner' by implementing technologies that enable us to work innovatively across organisational boundaries to improve services.

2 Why we need this policy

This policy sets out the Trust's procurement, re-assignment and disposal of IT & Telephony equipment.

2.1 Purpose

The purpose of this policy is to:

- Ensure that equipment is properly managed to support the provision of Trust services

- Assure to patients, carers and their families that our staff are using IT equipment that meets all required standards and ensures their information is kept safe and confidential.

- Ensure that any equipment is:
    - approved for compatibility for use with the Trust's systems
    - asset tagged; and
    - recorded on the Information Asset Registers within the Trust throughout its lifecycle.

- Ensure the security and integrity of the Trust's IT infrastructure,

- Ensure that no unauthorised or personal equipment or software is used within the Trust,

- Ensure that the Trust's Standard Financial Instructions (SFIs) and equipment purchasing eligibility criteria are adhered to.

- Ensure that the Trust's IT & Telephony equipment is re-assigned or disposed of in a secure and economically viable way.

2.2 Objectives

This policy aligns with Trust values by listening to staff and supporting their individual needs with regards to IT & telephony. The policy aims to ensure no staff member feels excluded by not having the right equipment to support their workplace adjustment when needed.

Adherence to this policy will ensure that:

- No unauthorised or personal equipment, or software, is used within the Trust, which could expose the Trust systems to unnecessary risk of security breaches, harm or failure. This is against the NHS Statement of Compliance and may instigate the Trust's disciplinary procedure.

- A standard list of equipment is maintained and updated within the Trust.

- Equipment used within the Trust is standardised, reducing the cost of purchase, installation, maintenance and training.

- Expertise in the use of equipment can be shared throughout the organisation more effectively, thereby increasing staff knowledge, accuracy and productivity and reducing costs.

- Safety of staff and service users and their information within the organisation is ensured.

- IT & Telephony equipment is asset tagged and registered with named owners, and that accurate records are kept in the appropriate Information Asset Registers.

- The Trust's SFIs are adhered to, ensuring the advice of the Trust's procurement advisers are taken into account in all instances to obtain maximum value for money.

- Access is made available to the necessary IT & Telephony equipment to allow staff and service users to carry out their tasks efficiently and effectively.

- Clear eligibility criteria, for the purchase of new IT & Telephony equipment, is available.

- IT & Telephony equipment is re-assigned or disposed of in a secure and economically viable way using the Trust's contracted suppliers to do so.

- IT & Telephony equipment is purchased by the Trust for the purposes of Trust business; any use of Trust equipment outside of this should be in line with the relevant manager's approval and in line with the Trust's associated approved usage policies.

- All IT & Telephony equipment procured, re-assigned or disposed of through the Information Service Desk will be processed in line with this policy.

3 Scope

This Policy applies to all Trust IT assets – defined as hardware and software.

3.1 Who this policy applies to

This policy is relevant to the following groups who use or have access to Trust IT & Telephony equipment, but is not limited to, these groups were initially consulted when the policy was developed.

- Staff
- Service Users
- Students
- Volunteers
- Budget Holders
- Line Managers

- Finance Services
- Information Services / Service Desk / Desktop Team
- Information Asset Owners / Information Asset Administrators
- External Suppliers

3.2 Roles and responsibilities

The following provides details of the roles and responsibilities of any user of Trust equipment including:

(Service Users have a separate policy and procedures covering their use and access to IT equipment and will liaise with clinical staff to deal with any issues which arise.)

Role	Responsibility
Staff, Students, Volunteers	• Abide by the principles and guidance contained within this policy and any Law pertaining to the use of IT & Telephony equipment. • Protect the IT & Telephony equipment against loss or theft, or inappropriate access or use. No equipment should be left unattended in an unsafe environment at any time and when not in use should be stored securely. • Report any inappropriate access or use of any item of IT & Telephony equipment, which may breach confidentiality, immediately through Datix and to the Information Service Desk if appropriate. E.g. to lock down the use or change passwords. • Report the loss or theft of any item of IT & Telephony equipment immediately through Datix and to the Information Service Desk and police. • Report faults via the Information Service Desk. (NB if it is shown that the fault was due to negligence by the user, the Trust reserves the right to pass these costs on to the user.) • Return any IT & Telephony equipment to the relevant line manager on leaving Trust's employment. If former members of staff fail to return any IT & Telephony equipment to the Trust they will be held responsible for all costs including data, calls and line rental and / or the replacement costs of the IT & Telephony equipment until it is returned and / or disconnected. • Read and adhere to this policy before requesting the procurement of any IT & Telephony equipment
Budget Holder / Line Manager	• Read and adhere to this policy before authorising the procurement of IT & Telephony equipment for users that meet the eligibility criteria. • Ensure IT & Telephony equipment is charged for by Finance and correctly allocated to their budget for any ongoing charges.

	• Ensure IT & Telephony equipment is used appropriately and that users understand and are aware of the relevant policies. • Ensure IT & Telephony equipment costs for repair/replacement are met out their budget. (NB if it is shown that the fault was due to negligence by the user, the Trust reserves the right to pass these costs on to the user.) • Ensure that all IT & Telephony equipment allocated to staff are recorded on the Information Asset Register (i.e. Encrypted data stick, mobile phone etc) and that the member of staff has sufficient knowledge of the device to use the equipment safely and in accordance with relevant Trust policies. • Ensure IT & Telephony equipment is managed in accordance with Trust policy, including the re-assignment, disposal and disconnection of any equipment to maintain security and reduce costs.
Information Asset Owners	• Ensure the Information Asset Register is kept up to date and that all asset numbers, descriptions and associated owners are recorded. They will ensure that any major changes are recorded, including when equipment is moved or decommissioned. • Will audit Information Asset Registers to ensure they are kept up to date and that all IT & Telephony equipment is properly utilised and recorded throughout the item's lifecycle including purchase, loss, and disposal.
Finance Service	• Ensure that periodic checks and trend analysis is carried out on all costs associated with IT & Telephony equipment and investigate high usage to ensure IT & Telephony equipment is being used appropriately.
IT Contracts and Asset Team	• Provide advice and guidance on Trust policy and procurement, re-assignment and disposal of IT & Telephony equipment. • Process orders received for the procurement, re-assignment and disposal of IT & Telephony equipment. • Act as a liaison point with the users, procurement service and suppliers for the procurement, re-assignment and disposal (and disconnection) of IT & Telephony equipment. • Ensure that the IT Equipment Inventory is updated with any changes made by external suppliers. • Ensure that the data quality of the IT Equipment Inventory is such that it can be used for tender exercises for third party contracts. • Ensure that items which are received by the Information Service Desk on behalf of users are asset tagged and recorded on the IT Equipment Inventory where appropriate e.g. Encrypted data stick • Ensure that Standard IT & Telephony equipment list is regularly reviewed and updated when required • Ensure that Standard IT & Telephony equipment represents value for money • Ensure all IT equipment returned is disposed of in a secure and safe manner in line with information security and solid waste management policies

End User Computer Manager and Network Manager	• Ensure that Standard IT & Telephony equipment meets the current needs of the Trust. • Ensure that Standard IT & Telephony equipment is aligned to the strategic direction of the Trust. • Ensure that Standard IT & Telephony equipment list is regularly reviewed and updated when required • Ensure that Non-Standard IT & Telephony equipment is tested for compatibility and security. • Conduct a regular verification exercise on the IT Equipment Inventory to ensure that it suitably reflects the Trust's requirements for maintenance and support. • Ensure that non-standard IT & Telephony equipment is assessed with the Trust's business strategy in mind to ensure it is aligned with the Trust's strategic direction. • Non-standard IT & Telephony equipment is assessed against the Trust's IT infrastructure and the Information strategy to ensure its compatibility. • Non-standard IT & Telephony equipment is assessed in accordance with Information governance.
External Suppliers	• Will supply IT & Telephony equipment as required and will ensure that timely delivery occurs to the correct destination. Where appropriate suppliers to the Trust will test all equipment, asset tag it and put a Trust image on to any item requiring one. • On a bi-weekly basis the third party installer will send details of all equipment installed to the Information Service Desk who will update the IT Equipment Inventory with the required details, ensuring it reflects the Trust's requirements for maintenance and support. • Ensure all IT & Telephony equipment returned to them is disposed of in a secure and safe manner in line with information security and solid waste management policies

4 Policy

4.1 Eligibility criteria

To procure, re-assign and/or dispose of IT & Telephony equipment within the Trust, the following criteria must be met:

4.1.1 Procurement

IT & Telephony equipment, including software, may be purchased if:

- part of a project overseen by Information Services which has been approved by the executive Management Group.
- from the standard list and is purchased with the budget holder's permission to carry out the work of the Trust.
    - Upgrades will only be provided if it is proven by the individual that an upgrade would be advantageous or at nil cost and is compatible with existing Trust systems.
- **not** on the standard list with the budget holder's permission to carry out the work of the Trust, **only** as recommended:
    - as part of a health and safety assessment
    - or disability reasonable adjustment assessment.
- from the standard list and with the budget holder's permission to carry out the work of the Trust, where the user needs regular use outside of the office in order to carry out duties. E.g.:
    - Member of either the Trust's Executive Team or the Board of the Trust
    - Member of an On-Call rota
    - The individual is required to be contactable, during normal work hours, where no fixed telephone system is available (e.g., when visiting clients' homes)
    - The individual does not have a main base, but utilises a 'Hot Desk' within the Trust, or is a home worker
    - The Individual is classified as a 'lone worker'
    - The individual is a mobile / community worker
    - There is a demonstrable requirement to keep in contact with the Trust, which is not covered above, where usage is not likely to be of an ad-hoc nature
    - At the discretion of the Chief Executive or Director of service.

Non-standard IT & Telephony equipment may be purchased if recommended as part of a health and safety or disability reasonable adjustment assessment.
Requests in this case must be formally logged with the Information Service Desk.

4.1.2 Re-assignment

- When a staff member moves team/leaves the Trust or changes job role, the relevant procedure must be followed. See:
  - IT **Laptop** Re-assignment or Disposal Procedure;
  - IT **Smartphones** Re-assignment or Disposal Procedure;
  - IT **Chargeable software** Re-assignment Procedure;

  as appropriate,

- IT & Telephony equipment, including software, may be re-assigned by budget holders/line managers using the same eligibility criteria as the procurement section of this policy.
- Where equipment/software is re-assigned, asset registers and budget cost codes must be updated to reflect the new location.
- Users who retain equipment but move to different locations or teams will need to ensure that the equipment is updated on relevant asset registers to remove and add details. Cost centres and budget codes will also need to be changed to ensure that the correct charges are being made to the appropriate services.
- Where a user takes a mobile phone or Mobile Working equipment with them to an alternative team, they must inform the Information Service Desk to ensure that the items can be tracked for usage.

Equipment such as mobile phones, computers and Mobile Working equipment, which have an ongoing cost for rental, maintenance or licensing, **must not be kept if not in use**.
These items **must be returned** to the Information Service Desk for re-assignment or disposal.

4.1.3 Disposal

IT & Telephony equipment, including software, must be:

- Disposed of in accordance with the Trust's Standard Financial Instructions (SFIs);
- Reported to the Information Service Desk for secure disposal in compliance with Information Security and Waste Electrical and Electronic Equipment (WEEE) disposal directives;
- Removed from the relevant Information Asset Register (IAR).

4.1.4 Restrictions

- Some items of a non-standard nature may be restricted to ensure that the Trust's systems are safe, secure, sustainable and provide a value for money.
- Availability of some items may be restricted whilst a Digital and Data Services project is underway or planned or where the cost of the item is significant enough to warrant restrictions, e.g. smartphones. If in doubt, contact the Information Service Desk for further information.
- Trust equipment cannot be purchased for personal use, unless it is purchased as part of a Service User's access to IT, under the Patient Access to the Internet policy.

4.1.5 Monitoring and Accounting Arrangements

- All costs associated with the use of IT & Telephony equipment will be included in the appropriate management budget reports. Budget holders are responsible for reviewing the IT & Telephony equipment and associated costs assigned to their cost centre. Some devices have an annual charge, which is reviewed and set in arrears. Current charges can be found on intranet.
- Periodic checks and trend analysis will be undertaken on all costs associated with IT & Telephony equipment by the Finance Department who will investigate high usage to ensure IT & Telephony equipment is being used appropriately.

- The Trust is not responsible for any cost associated with user home broadband connections, which may be used in conjunction with Trust equipment for work purposes.

4.2 Unauthorised equipment and software

The use of unauthorised equipment, software, or online tools puts the Trust's patient and staff information, infrastructure and assets at risk of disclosure, damage, or loss. The use of any unauthorised equipment, software, or online tools may result in disciplinary action.

4.2.1 Unauthorised equipment

Only authorised Trust issued equipment should be used for Trust business. This includes all equipment which will connect to the Trust network or existing Trust equipment (including all peripherals e.g,, keyboards, mice etc)

4.2.2 Unauthorised Software

The purchase and/or installation of all software is managed centrally and requests for the installation of **any** software must be submitted via the Service Desk Portal. This includes any software recommended as part of an Access to Work report or Reasonable Adjustment request. **No software that is unauthorised by the Digital and Data services may be used for Trust business. Any use of unauthorised software may result in disciplinary action.**

4.2.3 Unauthorised Online tools

Only approved online tools should be used for Trust business. The use of unauthorised online tools may result in data breaches and disciplinary action.

5 Definitions

The following terms and definitions are of use when reading this policy and related documents.

Term	Definition
Data Storage Device	• Any device which can store Personal Information, e.g. SIM cards, Mobile Phones, PCs, Laptops, etc. • These devices must adhere to the Information Security and Risk Policy and be protected and disposed in a secure manner.

	• Staff must only use Trust purchased equipment and encrypted laptops for business purposes.
InPhase	• InPhase is the Trust's incident reporting system. • If you are involved in or witness an incident, an InPhase incident report must be completed so that the incident can be investigated. • InPhase can be accessed via the Trust intranet.
Information Asset Administrator (IAA)	• IAAs ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management, and ensure that information asset registers are accurate and up to date.
Information Asset Owner (IAO)	• IAOs are senior individuals within the Trust. They are Associate Directors and General Managers / Heads of Service. • Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. • As a result, they are able to understand and address risks to the information; ensure that information is fully used both within the law and appropriately, and provide written input to the SIRO annually on security and use of their assets.
Information Asset Register (IAR)	• These are created by Information Governance (IG) and maintained by Information Asset Administrators (IAA) in consultation with their Information Asset Owner (IAO). IARs show what information assets are held and used by the team for which the IAA is responsible. • A record of all IT hardware and software that is used within the team/department must be held within the IAR, detailing all the hardware and software used, who uses it and where it is based including details of software licensing. • All mobile devices should be recorded and assigned to individual staff members. • The IAR needs to be kept up to date in real-time.
International Mobile Equipment Identity (IMEI)	• Each mobile phone is assigned a unique 15-digit IMEI code when it is produced. This stores the manufacturer, model type, date and country of approval.
IT & Telephony Equipment	• This includes hardware and software used by the Trust to conduct its business.
IT Equipment Inventory	• This is a list of IT equipment kept by Digital and Data Services for the management of support calls and third-party service contracts. • It is used solely by Digital and Data Services; it is not the formal IT equipment register for the Trust and will be updated as required for maintenance and support

	purposes e.g., when equipment is purchased or disposed of. • The IT equipment inventory will not possess real-time information on the location or ownership of IT equipment. This list is maintained by the third-party equipment suppliers and provided to the Desktop and Service Desk Managers on a regular basis.
Hardware	• Any equipment relating to IT or telephony such as: PC, Laptop, Monitor, Printer, Scanner, Server, Smart Phone, Mobile Phone, Desktop Phone, Digital Voice Recorders, Digital Image Recorders etc. • Some hardware enables the storage of confidential information and therefore careful consideration **must** be given to purchase, re-assignment and disposal.
Mobile Phone Provider	• The Trust contracts with one main mobile phone service provider to obtain best value for money. For technical reasons (e.g. poor coverage in some areas) an alternative mobile supplier may be used.
Non-Standard IT Equipment Item(S)	• Non-standard equipment items, including software, are IT equipment that do not appear on the IT Standard List available on either the Trust's intranet or Cardea. • A request must be formally logged with the Information Service Desk and explicit authorisation given after sufficient justification by the Information Service before any non-standard equipment can be purchased and introduced into the Trust. • Non-standard IT & Telephony equipment may also be recommended as part of a health and safety or disability reasonable adjustment assessment. • The Information Service Desk will ensure that any non-standard equipment purchased is compatible with the Trust's IT infrastructure, that it aligns with the Trust's business and that no security weakness will be introduced.
Portable media	• Any type of storage device which is capable of holding data and being transported around or out of the Trust. It can be in paper or electronic form.
Senior Information Risk Owner (SIRO)	• The SIRO is responsible for developing and implementing risk policy and making sure that it remains appropriate to the business objectives and the risk environment.
SIM Card	• Each mobile phone number has a unique SIM card associated with it. The SIM card is inserted into a mobile phone and provides the information required for connection to the mobile phone network. The SIM card can also store personal information such as phone numbers and other contact details.
Software	• Software is a general term for the various kinds of programs used to operate computers and related devices.

	• Some software enables the storage of confidential information and therefore careful consideration should be given to installation and removal.
Standard IT Equipment List	• This is the authorised list of all IT equipment items that are deemed standard to the Trust. These can be purchased without consultation. • A catalogue of larger standard items is shown on the Trust's intranet and can be ordered through the Information Service Desk. Smaller items can be ordered directly through the catalogue on Cardea.
Standard Financial Instructions (SFI's)	• SFIs detail the financial responsibilities, policies and procedures to be adopted by the Trust. • They are designed to ensure that the Trust's financial transactions are carried out in accordance with the law and Government policy in order to achieve probity, accuracy, economy, efficiency and effectiveness.
Trust Capital Asset Register	• This is a single asset register for all items that are valued at £5000 or more and are deemed an asset of the Trust.
Trust Procurement System	• This is the electronic system used to process requisitions within the Trust. The Trust currently uses Cardea as its electronic procurement system.

6 Related documents

The following procedures should be read with this policy as they relate directly to it:

- IT & Telephony Procurement Procedure
- IT Laptop Re-Assignment and Disposal Procedure
- IT Smartphone Re- Assignment and Disposal Procedure
- IT Chargeable Software Re-Assignment Procedure
- Information Security and Risk Policy
- Information Asset Register Procedure

7 How this policy will be implemented

This policy will be implemented in the following ways:

- This policy will be published on the Trust's intranet and external website.
- Line managers will disseminate this policy to all Trust employees through a line management briefing.

7.1 Training needs analysis

Staff/Professional Group	Type of Training	Duration	Frequency of Training
All Staff	Familiarisation with Policy	30 minutes	On commencing employment with the Trust
IAA (team / ward managers)	IAA Training	2 Hours	When allocated to the role.
Staff who receipt goods in Cardea	Cardea Training	60 minutes	When requiring access to Cardea

8 How the implementation of this policy will be monitored

Number	Auditable Standard/Key Performance Indicators	Frequency/Method/Person Responsible	Where results and any Associate Action Plan will be reported to, implemented and monitored; (this will usually be via the relevant Governance Group).
1	All requests for IT equipment are completed and the items issued within agreed timescales	Frequency = Monthly Method = supplier reports on equipment distributed Responsible = Central Asset Management Team	Digital & Data Architecture Group then Digital Performance and Assurance Group (DPAG)
2	Disposal Reports	Frequency = Monthly Method = suppler report on equipment disposal to ensure compliance with standards Responsible = Central Asset Management Team	Digital & Data Architecture Group then Digital Performance and Assurance Group (DPAG)

9 References

- ITAM Best Practice
- ITIL guidance

- National Cyber Security Group
- NHS England Data Security and Protection toolkit

10 Document control (external)

To be recorded on the policy register by Policy Coordinator

Required information type	Information
Date of approval	15 October 2024
Next review date	15 October 2027
This document replaces	IT-0020-v7 IT & Telephony Procurement, Reassignment and Disposal Policy
This document was approved	Architecture Group - 03 October 2024
This document was approved	DPAG – 11 October 2024
This document was ratified by	Management Group
This document was ratified	15 October 2024
An equality analysis was completed on this policy on	29 May 2024
Document type	Public
FOI Clause (Private documents only)	n/a

Change record

Version	Date	Amendment details	Status
6.0			Withdrawn
7.0	22 Sept 2021	Updated Introduction Responsibilities – Information Service Desk change to IT Contracts and Asset Team Some responsibilities moved from Desktop Product Manager to IT Contracts and Asset Team Responsibilities – Desktop Product Manager – changed to End User Compute Manager and Network Manager 4.1.1. Bullet point 4, sub point 4 - add or is a home worker 4.1.2 – point 4 main box and box 2 – word ‘dongles’ removed	Withdrawn
8	15 Oct 2024	Full review with the below changes: Removal of Implementation Plan	Ratified

		Amendments to KPI/monitoring tools Addition of links to new procedures Addition of section 4.2 - Unauthorised equipment and software Rewording of sections 1 & 2 Amendments to section 7 – bullet points moved to appropriate sections Amendment to the Governance Group that KPIs/performance is reported to	

Appendix 1 - Equality Impact Assessment Screening Form

Please note: The Equality Impact Assessment Policy and Equality Impact Assessment Guidance can be found on the policy pages of the intranet

Section 1	Scope
Name of service area/directorate/ department	Digital and Data Services
Title	IT Telephony Procurement Re-Assignment and Disposal Policy
Type	Policy
Geographical area covered	Trustwide
Aims and objectives	This policy has been created to ensure that staff and service users have easy access to clear information regarding the Trust's procurement, re-assignment and disposal of IT & Telephony equipment policy.
Start date of Equality Analysis Screening	May 2024
End date of Equality Analysis Screening	29 May 2024

Section 2	Impacts
Who does the Policy, Procedure, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan benefit?	Trust Staff, to allow them to order, re-deploy and dispose of Trust IT assets.
Will the Policy, Procedure, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan impact negatively on any of the protected characteristic groups? Are there any Human Rights implications?	• **Race** (including Gypsy and Traveller) **NO** • **Disability** (includes physical, learning, mental health, sensory and medical disabilities) **NO** • **Sex** (Men and women) **NO** • **Gender reassignment** (Transgender and gender identity) **NO** • **Sexual Orientation** (Lesbian, Gay, Bisexual, Heterosexual, Pansexual and Asexual etc.) **NO** • **Age** (includes, young people, older people – people of all ages) **NO** • **Religion or Belief** (includes faith groups, atheism and philosophical beliefs) **NO** • **Pregnancy and Maternity** (includes pregnancy, women / people who are breastfeeding, women / people accessing perinatal services, women / people on maternity leave) **NO** • **Marriage and Civil Partnership** (includes opposite and same sex couples who are married or civil partners) **NO** • **Armed Forces** (includes serving armed forces personnel, reservists, veterans and their families) **NO** • **Human Rights Implications NO** (Human Rights - easy read)
Describe any negative impacts / Human Rights Implications	n/a
Describe any positive impacts / Human Rights Implications	Staff will understand how they can obtain, redeploy and dispose of IT assets in the correct manner and where to seek guidance. By following the process, the Trust will use only approved equipment and dispose of IT assets in an approved manner. This in turn supports the Data Security and Protection toolkit and Cyber Security, assuring staff, patients, carers and families that the Trust takes seriously the protection of their personal data. The Policy also benefits staff who require a workplace adjustment by providing equipment that supports their individual requirements.

Section 3	Research and involvement
What sources of information have you considered? (e.g. legislation, codes of practice, best practice, nice guidelines, CQC reports or feedback etc.)	• ITAM (IT Asset Management) Best Practice • ITIL (Information Technology Infrastructure Library) guidance • National Cyber Security Group • NHS Digital England's Data Security and Protection Toolkit
Have you engaged or consulted with service users, carers, staff and other stakeholders including people from the protected groups?	No
If you answered Yes above, describe the engagement and involvement that has taken place	
If you answered No above, describe future plans that you may have to engage and involve people from different groups	No – as central asset management progresses, this policy will need to be re-written, as part of this work a wider consultation will be undertaken. The policy will be subject to a six week all staff Trustwide consultation

Section 4	Training needs
As part of this equality impact assessment have any training needs/service needs been identified?	No
Describe any training needs for Trust staff	n/a
Describe any training needs for patients	n/a
Describe any training needs for contractors or other outside agencies	n/a

Check the information you have provided and ensure additional evidence can be provided if asked.

Appendix 2 – Approval checklist

To be completed by lead and attached to any document which guides practice when submitted to the appropriate committee/group for consideration and approval.

Title of document being reviewed:	Yes / No / Not applicable	Comments
1. Title		
Is the title clear and unambiguous?	Yes	
Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2. Rationale		
Are reasons for development of the document stated?	Yes	
3. Development Process		
Are people involved in the development identified?	Yes	
Has relevant expertise has been sought/used?	Yes	
Is there evidence of consultation with stakeholders and users?	yes	6 week trustwide consultation to be undertaken at this version
Have any related documents or documents that are impacted by this change been identified and updated?	yes	
4. Content		
Is the objective of the document clear?	Yes	
Is the target population clear and unambiguous?	Yes	
Are the intended outcomes described?	Yes	
Are the statements clear and unambiguous?	Yes	
5. Evidence Base		
Is the type of evidence to support the document identified explicitly?	Yes	
Are key references cited?	Yes	
Are supporting documents referenced?	Yes	
6. Training		
Have training needs been considered?	Yes	
Are training needs included in the document?	Yes	

7. Implementation and monitoring		
Does the document identify how it will be implemented and monitored?	yes	
8. Equality analysis		
Has an equality analysis been completed for the document?	Yes	
Have Equality and Diversity reviewed and approved the equality analysis?	Yes	
9. Approval		
Does the document identify which committee/group will approve it?	y	Architecture Group then DPAG, then MG
10. Publication		
Has the policy been reviewed for harm?	Y	No harm
Does the document identify whether it is private or public?	y	Public
If private, does the document identify which clause of the Freedom of Information Act 2000 applies?	n/a	
11. Accessibility (See intranet accessibility page for more information)		
Have you run the Microsoft Word Accessibility Checker? (Under the review tab, 'check accessibility'. You must remove all errors)	Y	
Do all pictures and tables have meaningful alternative text?	Y	
Do all hyperlinks have a meaningful description? (do not use something generic like 'click here')	y	