Tees, Esk and Wear Valleys
NHS Foundation Trust

Public – To be published on the Trust external website

Digital and Data Contract Management Policy

Ref: IT-0036-v1

Status: Ratified
Document type: Policy

Contents

1 Introduction

The purpose of this Digital and Data (D&D) Contract Management Policy is to provide a clear and standardised approach to managing and administering Digital and Data contracts for goods, services and works purchased from suppliers. It also sets out what elements should be included in D&D contracts prior to contract award and signature, including the due diligence checks around Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR) requirements including Data Protection Impact Assessment (DPIA).

This policy applies to any electronic system, hardware, service, or software in use by the Trust, referred to collectively as Digital and Data, regardless of the service that has been identified as Business or Service owners.

1.1 Strategic goal 1: To co-create a great experience for patients, carers and families

By ensuring the Trust has robust Digital and Data contract management in place and ensuring contracts have the necessary clauses in around Data Protection Act 2018, UK GDPR, Cyber Security etc, the Trust can provide assurance to patients, carers and their families that our Digital and Data systems and equipment meets all required standards and ensures their information is kept safe and confidential and systems are fit for purpose.

1.2 Strategic goal 2: To co-create a great experience for our colleagues

This policy ensures that colleagues understand their role around the lifecycle of Digital and Data contracts, what elements must be included to ensure robust contracts are in place. The contract provides details of where to obtain support in their development, in what can often be a new area for colleagues, so provides them with the assurance and support they need.

1.3 Strategic goal 3: To be a great partner

Digital and Data systems, hardware, software etc are key to the services that the Trust provides, to maximise the benefit, good relationships must be created with suppliers and other partners. By having a policy that clearly defines how the Trust will manage its Digital and Data contracts, and what will be included, this provides partners with a clear view on how the Trust will engage with them.

1.4 Trust Values and behaviours

Embedding good contract management practices enables us to evidence how we live our values of respect, compassion and responsibility in everything we do.

2 Why we need this policy

Electronic Systems, hardware, services and software (Digital and Data) can be complex, and the Trust has an ever-increasing reliance on technology. As such it is vital that the Trust has robust contracts and contract management in place.

This policy applies to all electronic system, hardware, services and software in use by the Trust, regardless of the service identified as the Business or Service Owner. This is to ensure all such systems, services, hardware and software comply with the Trust and national standards around security, compliance etc.

Governance – This policy ensures staff are aware of the necessary governance required for the procurement of any Digital and Data system/solution and that the approval of Digital Programme Board (DPB) or Digital Programme Assurance Group (DPAG) is sought.

Digital and Data Contract Management enables the Trust and its suppliers to meet their contractual obligations at an agreed cost and quality by monitoring the contract throughout its lifecycle. Circumstances may change over the life of a contract, so contract management also involves managing changes and variations in terms of scope, terms, and prices. It also enables appropriate contract forward planning to ensure that the Trust achieves its objectives, and that procurement takes place in a structured way in compliance with the law and the Trust's rules.

The effective management of Digital and Data contracts with suppliers is essential to the Trust in maximising the benefits and achieving its objectives

2.1 Purpose

The purpose of this policy is to ensure:

- Standard approach is undertaken to Digital and Data contract management
- Compliance with legislative and administrative arrangements
- All details, terms and clauses required under Data Protection Act 2018 and UK GDPR are included
- Digital and Data Contracts are managed in a manner that facilitates business delivery while minimising Risk
- Contracts are managed maximising financial and operational performance
- All staff are adequately skilled and trained and understand their roles and responsibilities under a contract.
- Approval from the relevant group (DPB/DPAG) is sought prior to any procurement and contract signature.
- New Digital and Data contracts, have all the necessary clauses in place.
- The Trust uses only endorsed framework agreements
- The Trust's Standard Financial Instructions (SFIs) and equipment purchasing eligibility criteria are adhered to.

- The Trust can meet the requirements around contracts and suppliers in the Data Security and Protection Toolkit (DSPT)

2.2 Objectives

Adherence to this policy will ensure that:

- Digital and Data contracts are effectively managed thorough the full life cycle
- Staff understand their responsibility in Digital and Data contract management
- The terms and conditions for Digital and Data contracts contain all the required clauses
- Only endorsed framework agreements are used
- The necessary due diligence has taken place prior to contract signature
- Understand the phases of Digital and Data contract management
- Contract managers/system owners are clear on financial authorisation limits
- Compliance with the DSPT

3 Scope

This Policy should be read prior to the award of contract for any Electronic System, Hardware, Service or Software to ensure all relevant clauses are incorporated and the necessary due diligence checks are carried out. These will then be used in the Post-Contract-Award stage of the Procurement Lifecycle. The procurement is covered in the Trust's Financial Standing Instructions.

Advise should be sought from the Digital and Data Departments Contracts Manager, and the Procurement service on how to procure services.

This policy is relevant to the following groups

- Staff
- Business Owners
- Service Owners
- Technical Owners
- Contract Manager(s)
- Budget Holders
- Line Managers
- Finance Services
- Digital and Data Services
- External Suppliers

3.1 Roles and responsibilities

The following provides details of the roles and responsibilities:

Role	Responsibility
Digital and Data Dept: Contracts Manager	• Ensuring D&D contracts prior to award contain all necessary clauses. • Ensuring D&D Contracts are registered in the Digital and Data and Trusts contracts register. • Maintaining a repository of all D&D contract related documentation • Day to Day management of assigned contracts • Clearly defining the performance standards, review mechanisms and deliverables required from contractors • Setting the standards and framework, for ensuring contracts are managed in compliance with approved policies, procedures and processes and all client obligations contained in contracts are fully satisfied. • Informing Business/Service/Contract owners in a timely manner of contract end dates and assisting with contract extensions and re-procurement. • Communicating with Finance, to ensure the Digital and Data contract register is aligned with the Trust wide contract register
Contract Manager/Service Owner	• Day to Day management of assigned contracts • Carrying out Service review meetings • Monitoring service delivery and performance against set SLA's • Documenting all Service review meetings • Clearly defining in contracts, the performance standards, review mechanisms and deliverables required from contractors • Reviewing contract variations • Communicate updates with finance to ensure all contracts are included on the Trust wide contract register
Business Owner	• Authorisation of any variations and extensions • Seeking assurance that the contract is performing and being monitored • Appointing the Contract Manager/System Owner
Technical Owner	• Assisting the Service owner in defining specification for contract • Supporting with procurement exercises and managing items outlined in the contract such as licence payments • Reviewing any technical elements of change notices
Finance Service:	• Ensuring Digital and Data contracts are recorded in the Trust wide contract register • Budget approval for renewals, variations, and extensions • Providing advice on contract financial elements • Maintaining Trust wide contract register

	• Escalation Point / Primary Contact for liaison with procurement services
Digital and Data Dept: Contracts Team	• Maintaining the Digital and Data Contracts register, including the filling and collation of all contract related documents. • Producing reports on Digital and Data contracts • Monitoring contract end dates • Processing requisitions for contract annual fees, variations, and extensions via the Trusts procurement system
Procurement Services	• Providing support during procurement • Providing advice and guidance on contract term values, variations, and extensions • Processing requisitions via Cardea • Issuing Contract Extension questionnaires • Issuing formal extension letters
Legal Partners	• Providing advice on terms and conditions • Supporting contractual disputes

4 Policy

4.1 Digital and Data Contract Management

The function of Digital and Data contract management is the management of Digital and Data contracts formed with Contractors to ensure delivery of goods, services, and works as agreed over the life of the Contract.

The management of a Digital and Data contract may extend beyond the current term of the contract when there are ongoing obligations associated with maintenance agreements, warranties and guarantees.

4.1.1 Stages in Digital and Data Contract Management Life Cycle

- Stage 1 - Contract Commencement: How to initiate and plan the contract management process
- Stage 2 - Contract Management: How to manage and administer contracts
- Stage 3 - Contract Close Out: How to close and transition contracts

Stage 1 – Contract Commencement: Starts Before the Contract is Signed.

- Successful Contract Management is highly influenced by activities performed prior to contract award.
- Ensuring that due diligence, contract terms, conditions, scope, and deliverables, KPI reporting, and relationship management are clearly established in the signed contract and understood by all parties, is fundamental for effective Contract Management.

Stage 2 - Contract Management – Runs until formal closure

- Properly managing supplier performance with respect to outcomes and deliverables clearly specified and agreed in the contract, will help ensure the Trust and its service users obtain the business benefits and value for money within target timeframes.

Stage 3 - Contract Closure – The formal conclusion

- The contract close-out is the stage for closing-out Contract obligations and liabilities with suppliers.
- It may also include transitioning to another supplier for the goods, services or works.
- Ensure any lessons learnt are recorded

> ! It is vital that the pre-contract sign activities are carried out and that the terms and conditions cover all key areas, once the contract is signed these can only be amended by variation, on agreement of both parties.

4.1.2 Mandatory Requirements applying to Digital and Data Contracts

The following minimum requirements apply to all Trust Digital and Data Contracts.

- **Staff must ensure that the purchase of Digital and Data goods and services is carried out in line with the Trusts standing financial instructions**

- **Specific contract details must be entered into Trusts Digital and Data Contracts Register, this is maintained by the Digital and Data Departments Contracts Management Team**

- **A Contract Manager/Service Owner must be formally appointed (Mandatory).**
  - The Contract Manager/Service Owner may manage a contract valued at more than their level of financial delegation. However, the Contract Manager/Service Owner must not approve or incur expenditure on goods, services or a project valued at more than their level of financial delegation. Note, this also applies to any changes (variations) to the original price of procurement.

- **Contract Regulations**
  - The Trust must comply with the Public Contracts Regulations 2015 where they are applicable.

- **Terms and Conditions**
  - NHS or endorsed framework terms and conditions should be used whenever possible
  - Specific advice should be sought from the Digital and Data depts Contracts Manager or the Trust legal partners during the planning stages of procurement to determine the appropriate terms and conditions that should apply.

- **Frameworks**
  - Where a framework is to be used, it must be one of those endorsed by NHS England and NHS Improvement as set out in the Procurement Framework Strategy Recommendations
  - The Trust should use these framework agreements for all digital buying. This will support and encourage both commercial best practice and innovation in the market and help reduce unnecessary transaction costs.
  - The Frameworks endorsed will use the Framework terms and conditions, these cannot be altered, but a range of schedules are included that can be amended to include the Trust's requirements.
  - Where it Is agreed not to use one of the endorsed framework agreements, this must be signed off at a senior level, and a rationale for the decision recorded.

⚠	Use of non-endorsed Frameworks are likely to prevent the Trust accessing shared or central funding for the services in question. Any increased risks of supplier performance or unwarranted costs incurred because of this will be the Trusts sole responsibility.

- **Data Protection Impact Assessment (DPIA)**

  More details can be found in the Data Protection Impact Assessment (DPIA) procedure, but:

  - A DPIA must be undertaken prior to any contract award, using the Trust's DPIA Form
  - The DPIA should be completed by the person responsible for the contract
  - It is advisable to include the following in the completion of this form:
    - Trust Data Protection Officer (DPO) and Information Governance Team
    - Relevant stakeholders
    - Digital and Data & Information Security Team
    - Any data processors (including 3rd party suppliers)
    - Legal advisors or other subject matter experts, where relevant

  - The DPIA supports the NHSE/I Digital Technology Assessment Criteria (DTAC) as part of the due diligence process.

- Following completion of the DPIA, it may also be necessary to consult with the Information Commissioner's Office (ICO) where measures cannot be taken to reduce any residual high risk of implementation.

- The DPIA must be approved and signed by the organisations Data Protection Officer (DPO)

⚠	DPIA: This is a mandated legal requirement of Data protection legislation to ensure the privacy concerns have been considered and actioned to ensure the security and confidentiality of personal identifiable information.

- **Data Protection Act 2018 and UK GDPR clauses must be included in Digital and Data contracts, these must cover these must include as a minimum:**
  - Processing only on the documented instructions of the controller.
  - Duty of confidence.
  - Appropriate security measures.
  - Using sub-processors.
  - Data subjects' rights.
  - Assisting the controller.
  - End-of-contract provisions.
  - Audits and inspections

The Trust's Information Sharing Procedure should also be consulted

Further advice and guidance can be sought from the Trust's Head of Information Governance

- **Cyber Security clauses/requirements – Digital and Data Contracts must contain clauses to cover the following:**
    - Penetration Testing approach for the supplier (annual as a minimum with evidence to support remediation of any vulnerabilities affecting the contracted system/s and or application/s)
    - Software and Hardware Patching of the system/s and application/s– frequency and responsibilities
    - Minimum standards required, ISO 27001, Cyber Essentials, Use of Multi-Factor Authentication (MFA) to secure infrastructure/hosted software, load testing has been performed.
    - Audits and inspections
    - Disaster recovery/business continuity
    - Clearly outline the responsibilities of the Trust and Supplier
- Further advice on cyber security can be sought from the Technical Delivery Manager

- **Hosted Systems/Services must contain clauses to cover the following:**
    - Cloud Native with UK based hosting location(s)

- **Clinical Software/SaaS/Apps must contain clauses to cover the following:**
    - NHS Number as core data Record
    - Web based user interface
    - Open Application Programming Interfaces (API)
    - HL7 Compliant
    - FHIR Standard Compliant
    - DCB0129 Compliant
    - SNOMED CT and/or ICD10 Compliant

- **All Contracts must include appropriate clauses in the areas of:**
    - Green, Carbon Net Zero
    - Ethical/Sustainability
    - Equality and Human Rights (Compliance with Equality Act 2010 and Human Rights Act 1998)
    - Social Values
    - Modern Slavery
    - Work Health & Safety
    - Quality Assurance
    - Environmental
    - Financial Capability
    - Insurance
    - Industrial Relations
    - Performance
    - Code of Conduct

- **Performance Clauses**

- Contracts should be clear on how performance will be monitored at all stages, including implementation, go-live and decommissioning. They should also include any reference to penalties associated with poor performance.
- Clauses should be included to allow for termination of Contract for failing to meet set performance levels

- **Intellectual Property Rights (IPR)**
  - Where contracts contain areas that will fall under IPR, such as the development of systems, processes etc. Then appropriate IPR clauses MUST be included within the contract. It is recommended that legal advice is sought in this area.

- **Commercial Clauses: All contracts must include appropriate clauses in the areas of:**
  - Payments and Retentions (or security)
  - Price Adjustments
  - Delay to Completion (or delivery)
  - Processes to Resolve Claims and Disputes.

- That allow managing or regulating variations to the original contract, having regard to project value, contract requirements and complexity.

- **Contract Performance of all Contracts must be regularly monitored**
  - The frequency will depend on the criticality of the contract and its value.
  - Notes should be kept of any service review meeting, along with any performance reports

- All documents and notes associated with the monitoring of the contract, should be kept in the Digital and Data contract system

- **Exit Strategy – All contracts should include an Exit strategy/plan, the following areas should be considered, when developing.**
  - Continuing Service Requirements
  - Data, Security and Privacy including
    - Safe Data return and/or Evidence of destruction
  - Knowledge and Documented Transfer
  - Costs
  - Personnel

> ! Failure to apply the mandatory requirements, could lead to issues during the life of the contract.

4.1.3 Contract Variation

- All Contract Variations must be approved in writing in accordance with the contract and be approved by the appropriate delegate (who has the authority to sign for the level of expenditure in the variation) and a formal Deed of Variation completed to reflect the change. All variations MUST be forwarded to Digital and Date Departments Contracts team. Signed copies of the Variation form, must also be included on the procurement system when raising associated purchase orders

- Contract Variations must be formally agreed via a variation form or change control notice (CCN). Most contracts should include a template that covers variation/change.
- The overall financial value of the contract for the term must be taken into consideration, to ensure the variation does not exceed the permitted financial value of the contract.

4.1.4 Contract Extensions

- Contract extensions must be agreed, following the Trust's internal governance route, and a contract extension request form must be completed.
- Sufficient notice as set out in the contract must be given to the supplier in order to exercise the extension option.

4.1.5 Code of Conduct

- The Trust's Employee Code of Conduct must always be adhered to in the management of contracts on behalf of Trust.

5 Definitions

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

Term	Definition
Digital and Data Contract	• An agreement, exchange of letters, heads of agreement, deeds of agreement, binding memorandum of understanding, response to tender, grant application, trust deed and any other document which creates, or which may create binding obligations on the Trust and on the other party / parties to the contract. This relates to IT systems, software, hardware, and services
Contract Management	• Refers to all activities at the commencement of, during and after the contract period, to ensure that all contractual obligations have been completed.
Digital and Data Dept: Contacts Manager	• The Trust staff member, who is responsible for maintaining the Digital and Data Contracts register, providing advice and guidance on contract management and producing contract reports.
Contract Owner	• The Trust staff member who is ultimately accountable for the outcomes of the contract, usually the Director of Finance, Chief Information Officer or Head of Service with the Delegated Authority. The Contract Owner approves contract variations, including extensions, as well appoints the contract management roles.

Contract Manager	- The Trust's staff member nominated to be responsible for the management of the administration and management of a contract.
Service Owner	- The Person responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a product, service, system, or application. It is not usually a technical engineer / developer. They are responsible for the operation and availability of the product, system, or application.
Business Owner	- The Trust staff member responsible for the part(s) of the Trust where the system or application is critical and is within their responsibilities and are responsible for its funding. This role is normally someone at a senior management level.
Technical Owner	- This is subject-matter expert who uses their technical background to bridge the gap between the product and technical side of product, system, or application. It is the person who will lead and coordinate on any technical changes, configuration, and updates and ensure that backups are working, and the system is secure. This most often someone within the Digital and Data Department
Digital and Data Contract Register	- A register maintained for all Digital and Data Contracts
Contract Variation	- Is an addition or alteration to the original contract and may include a change to the scope of the contract, value of the contract, the contract options to be exercised, contract prices and quantity purchased.
Contract Extension	- Where the contract states that it may be extended by its initial term. Contracts may not be extended beyond the initial term, unless it clearly states there are extension options.
Contractor	- The supplier or the service provider (the other party) under a contract.
Value of a Contract	- The value of a contract is whichever of the following values is appropriate to the kind of contract concerned: • The total estimated value of the project, or • The total estimated value of the goods, services or works over the term of the contract
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.

Procurement Services	- Services provided by CDDPS Services, to provide procurement expertise.
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.
DSPT	- Data Security and Protection Toolkit (DS&PT) an annual self-assessment for health and care organisations. It shows what is required to keep people's information safe and to protect the organisation from the risk of a data breach or a cyber-attack.
Public Contract Regulations 2015	- Outlines the rules on purchasing of goods and services by public sector bodies
Procurement Framework Strategy Recommendations	- Guidance developed by NHS England and NHS Improvement, to help simplify the digital and IT framework landscape, remove duplication, and reduce cost.
DPIA	- Data Protection Impact Assessment (DPIA) is a mandated legal requirement of data protection legislation to ensure that privacy concerns have been considered and actioned to ensure the security and confidentiality of the personal identifiable information.
UK GDPR	- UK General Data Protection Regulation (UK GDPR) – is how personal information is used by organisations, business, and the government. The Data Protection Act 2108 is the UK's implementation of the GDPR.
ISO27001	- International standard on how to manage information security
Cyber Essentials Plus	- UK Government backed, industry-supported certification scheme to help organisations demonstrate operational security against common cyber-attacks.
SaaS	- Software as a Service (SaaS), a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted.
API	- Application programming interface (API), which is s set of definitions and protocols for building and integrating application software.
HL7	- High Level 7 (HL7) is a set of international standards for the transfer of clinical and administrative data between software applications used by healthcare providers
FHIR	- Fast Healthcare Interoperability Resources (FHIR) is the global industry standard for passing healthcare data between systems
DCB0129	- This standard provides a set of requirements suitably structured to promote and ensure the effective application of clinical risk management by those organisations that are responsible for

	the development and maintenance of Health IT Systems for use within the health and care environment
SNOMED CT	• SNOMED CT is a structured clinical vocabulary for use in an electronic health record. It is the most comprehensive and precise clinical health terminology product in the world.
ICD10	• The International Statistical Classification of Diseases and Related Health Problems 10th Revision (ICD-10) is produced and maintained by the World Health Organisation (WHO). It was first mandated for use in the UK in 1995.

6 Related documents

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

- Standing Financial Instructions
- Introduction of information systems
- Information Security and Risk Policy
- Data Protection Impact Assessment (DPIA) procedure
- Information Sharing 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
Contract Manager and System owners	Contract management training	TBC	Annually

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	New contracts include mandatory clauses/information around GDRP, Cyber Security, Performance and Payment Terms	**Frequency:** Quarterly **Method**: Review prior to contract signature and update Quarterly contract report file **Person Responsible**: Digital and Data: Digital and Data Contracts Manager	Digital Performance and Assurance Group (DPAG)

9 References

Data protection: The Data Protection Act

NHS Digital Procurement Framework Strategy recommendations

Public procurement policy

NHS terms and conditions: procuring goods and services

The Public Contracts Regulations 2015

Guide to the UK General Data Protection Regulation (UK GDPR) | ICO

Data Security and Protection Toolkit

Cyber Essentials - National Cyber Security Centre

10 Document control (external)

To be recorded on the policy register by Policy Coordinator

Date of approval	15 February 2023
Next review date	15 February 2026
This document replaces	n/a – new document
This document was approved by	Digital and Data Management Meeting (DDMM) Digital Performance and Assurance Group (DPAG)
This document was approved	DDMM – 24 January 2023 DPAG – 01 February 2023
This document was ratified by	Management Group
This document was ratified	15 February 2023
An equality analysis was completed on this policy on	17 August 2022
Document type	Public
FOI Clause (Private documents only)	n/a

Change record

Version	Date	Amendment details	Status
1	15 Feb 2023	New document	Ratified

Appendix 1 - Equality Analysis Screening Form

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

Section 1	**Scope**
Name of service area/directorate/department	Finance and Information
Title	Digital and Data Contract Management Policy
Type	Policy
Geographical area covered	Trust-Wide
Aims and objectives	Digital and Data Contract Management Policy is to provide a clear and standardised approach to managing and administering Digital and Data contracts for goods, services and works purchased from suppliers. It also sets out what elements should be included in Digital and Data contracts prior to contract award and signature, including the due diligence checks around DPIA and GDPR.
Start date of Equality Analysis Screening	30 April 2022
End date of Equality Analysis Screening	10 June 2022

Section 2	**Impacts**
Who does the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan benefit?	Anyone who works on behalf of the Trust in the procurement, award, management and termination of Data and Digital contract.
Will the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan impact negatively on any of the protected characteristic groups?	• **Race** (including Gypsy and Traveller) **NO** • **Disability** (includes physical, learning, mental health, sensory and medical disabilities) **NO** • **Sex** (Men, women and gender neutral etc.) **NO** • **Gender reassignment** (Transgender and gender identity) **NO** • **Sexual Orientation** (Lesbian, Gay, Bisexual and Heterosexual 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 who are breastfeeding and women 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**
Describe any negative impacts	None Identified
Describe any positive impacts	This Policy ensures that all Trust Digital and Data contracts must contain clauses around Ethical/Sustainability, Social Values, Modern Slavery and compliance with Equality Act 2010 and Human Rights Act 1998 Ensuring the Trust is inclusive and diverse in the contracts it awards for its Digital and Data services.

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.)	Public Procurement Policy Public Contracts Regulations 2015 NHS Digital Procurement Framework strategy recommendation ICO's guide to UK GDPR National Cyber Strategy 2022
Have you engaged or consulted with service users, carers, staff and other stakeholders including people from the protected groups?	Yes
If you answered Yes above, describe the engagement and involvement that has taken place	This policy has undergone Trust-wide consultation. Trust staff comprise all the protected characteristics.

	Also this policy is based on ‘Public Procurement Policy’ which underwent significant national consultation.
If you answered No above, describe future plans that you may have to engage and involve people from different groups	Not Applicable

Section 4	**Training needs**
As part of this equality analysis have any training needs/service needs been identified?	No
Describe any training needs for Trust staff	None
Describe any training needs for patients	None
Describe any training needs for contractors or other outside agencies	None

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

Appendix 2 – Approval checklist

	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	
	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**		

	Title of document being reviewed:	Yes/No/ Not applicable	Comments
	Has an equality analysis been completed for the document?	Yes	
	Have Equality and Diversity reviewed and approved the equality analysis?	Yes	17th August 2022
9.	**Approval**		
	Does the document identify which committee/group will approve it?	Yes	
10.	**Publication**		
	Has the policy been reviewed for harm?	Yes	
	Does the document identify whether it is private or public?	Yes	public
	If private, does the document identify which clause of the Freedom of Information Act 2000 applies?	N/A	