

Introduction or Upgrade of Information Systems Procedure

Ref IT-0032-001-v2.2

Status: Approved

Document type: Procedure

Contents

1	Purpose	3
2	Related documents	3
3	Procedure	3
3.1	Develop the concept: consider the need	3
3.2	Governance Groups: Strategic alignment	4
3.3	From concept to approved business case.....	6
3.4	Implementation	6
3.5	Transition to Operations in Information Department.....	7
3.5.1	Checklist	7
3.5.2	Assurance	8
4	Definitions	8
5	References	9
6	Document control	10
Appendix 1: Process model for Form 0 to Form 3		11
Appendix 2 – OSI Seven-Layer Model		12
Appendix 3 - Equality Analysis Screening Form		15

1 Purpose

It is essential that we identify any potential resource requirements for new or upgraded information systems to help us target our means towards the developments that will achieve the most benefits for the business and our customers.

Following this procedure will help the Trust to:-

- Introduce a new information system that is fit for purpose
- Upgrade existing information systems

2 Related documents

This procedure describes what you need to do to implement the Introduction or Upgrade of information Systems procedures section of the Maintenance of IT Systems Policy [ref IT-0032].



The Maintenance of IT Systems Policy defines the principles which you must read, understand and be trained in before carrying out the procedures described in this document.

This procedure also refers to:-

- ✓ Information Security and Risk Policy [ref IT-0010]

3 Procedure



The Information department will not accommodate any system developments pursued outside of the process described in this document

New developments must adhere to the following stages from concept to implementation:

3.1 Develop the concept: consider the need

When considering new ideas, consult with all key stakeholders. In the case of information systems, you must include the Information department as part of this stakeholder group. The Supporting Users Team should be contacted to support for ideas or proposals at this stage of development.

Focus on:

- What is the information need or gap?
- What would be the business benefits of meeting this need?
- Can current practice be improved without a new system?

- Equality Analysis – ensuring that the needs of people with disabilities and other protected groups are considered.

When you have established a clear need, the Heads of Information will present a Form 0 to Digital Transformation Board for consideration.

3.2 Governance Groups: Strategic alignment

Any developments must be clearly identified in the Trust’s business plan. The following groups provide the governance for information system developments:

Group	Responsible for
Digital Transformation Board	<ul style="list-style-type: none"> • The programme board governing the delivery of the Digital Transformation programme’s projects and workstreams. • The aim of the board is to implement the Digital Transformation Strategy in the Trust to ensure that the Trust’s digital transformation vision is achieved.
Digital Safety and Information Governance Board	<ul style="list-style-type: none"> • Promoting and ensuring that effective clinical risk management is carried out prior to deploying, developing and modifying health IT systems.
Managing the Business Group	<p>The aims of the groups include:</p> <ul style="list-style-type: none"> • reviewing the quality of data produced within the organisation, ensuring there is a culture of continuous improvement in the quality and accuracy of the information • providing assurance to stakeholders that information reports are accurate and reliable • providing effective communication and engagement with Trust stakeholders and Trust staff on data quality and use of information • Any issues that require further senior approval or support will be escalated to Director of Planning and Performance and/or the Director of Finance and information
Cyber Security	<ul style="list-style-type: none"> • To receive up-dates from key functional areas within the Information Department & Information Governance team in relation to the Cyber security activities. This would include: <ul style="list-style-type: none"> ○ Information incidents ○ Third party audits ○ Penetration schedule of events ○ Identification and review of critical systems to include Business Continuity Plans (BCP) and Disaster Recovery (DR) ○ Desktop security alerts ○ Technology Alerts ○ Review & prioritisation of care cert actions

3.3 From concept to approved business case

Annually, the Digital Transformational Board (DTB) and the Executive Management Team (EMT) agree the priority schemes for the coming year's Trust Information Strategy.

Business-critical proposals may be considered in-year by either the DTB or Managing the Business Group (MBG) and EMT.

All approved proposals will need a detailed business case using the Trust's project management framework.

Document	Contents
Form 1	Scope of the development Request resources for requirements gathering Market review Stakeholder consultation Development of Form 3
Form 3 (Outline Business Case)	Outline scope Identify detailed benefits Implementation timescales Implementation plan Project Initiation document (PID) Plans for procurement Quality impact Assessment Data Protection Impact Assessment Equality Analysis – this must be considered from requirements gathering onwards i.e. it should not be done at the end
Form 3 (Full Business Case)	As for OBC but post-procurement How the development supports the Trust's strategic vision Which of the Trust's objectives the development will address Expected outcomes and benefits of implementation Identify all costs including capital and recurring expenditure

These forms must be presented to and considered by relevant governance group before going to EMT for approval.

3.4 Implementation

Approved schemes are monitored by the relevant governance group and reported each month as part of the Trust's project management framework to EMT.

Introduction of new information systems or upgrades to existing systems should be delivered using project management methodologies and principles.

Project implementation plans must establish and monitor:

- Agreed timescales
- Appropriate resources
- Impacts on other systems
- Impacts on stakeholders

For the introduction or upgrade of clinical systems, assurance is required that the skills, competence, capacity and confidence to take on the system are present, otherwise clinical safety may be compromised or benefits might not be realised. To ensure that clinical safety is not compromised, a Pilot site approach should be considered to evaluate any risk to patient safety before any large scale implementation is undertaken.

3rd party audits will be undertaken as required by the Information Security Officer. Transition of the new or upgraded system to the services that will use it as opposed to transition to IT Operations (covered in section 3.5) is an important aspect of the project implementation. Staff who will be using the system should be engaged in the process at the earliest possible stage. This will enable the staff to identify any possible areas of improvement that maybe required before it goes live.


The training needs for users must also be carefully considered, taking into account how they can demonstrate practical competence in using the system.

All developments of new web and browser systems should consider meeting the Worldwide Web Consortium (W3C) Web Content Accessibility Group (WCAG) 2.0 AA standard. There are three potential levels of WCAG compliance ranging from A-AAA, with A being the minimum required to ensure a website does not contravene the Disability Discrimination Act (2005) and AAA defining the requirements for a site specifically designed to support users with impaired motor, visual, or auditory capabilities.

Developments in non-Web technologies will consider Guidance on Applying WCAG 2.0 to Non-Web Information and Communications Technologies.

3.5 Transition to Operations in Information Department

3.5.1 Checklist

Task	Responsibility	Done 
Project Documentation Form 3 Outline Business Case Form 3 Final Business Case (if relevant) Contractual agreements Equality Analysis Final copy of project AIR log PM4 including Benefits Data Protection Impact Assessment signed off by Data Protection Officer	Project Manager	
Operational and technical documentation e.g.	Project Manager	

IP Address allocation PC Imaging Procedure Asset Register for items deployed as part of the project Server documentation Process for ordering new equipment, including costs Maintenance process		
Named system owner agreed	Project Manager	
Product Catalogue entry including how items are purchased	Project Manager	
Service Desk script(s) written and signed off	Project Manager	
Training for Operational support staff	Project Manager	
Training approach and material for system/product users e.g. E-Learning modules	Project Manager	
End user documentation e.g. How to User Instructions	Project Manager	
System Specific Policy to include agreed processes for the safe and legal governance, support, backup plans and maintenance arrangements for the system	Project Manager	

3.5.2 Assurance



Systems must not transfer to live operation until the System Specific Policy is approved

All systems require a System Specific Recovery Plan; for this, system owners should refer to the Information Systems Business Continuity Policy.

4 Definitions

Term	Definition
Stakeholder	<ul style="list-style-type: none"> Anyone who has an interest in the operation of the system, or the output from the system or from benefits derived from the system
System Owner	<ul style="list-style-type: none"> An individual with managerial responsibility for the system
Information system	<ul style="list-style-type: none"> An integrated set of components for collecting, processing and storing data and for delivering

	information
EMT	<ul style="list-style-type: none">• Executive Management Team
Clinical Safety Officer	<ul style="list-style-type: none">• Individual responsible for assessing the clinical safety of Patient systems to ensure that clinical safety of patients is not put at risk

5 References

None.

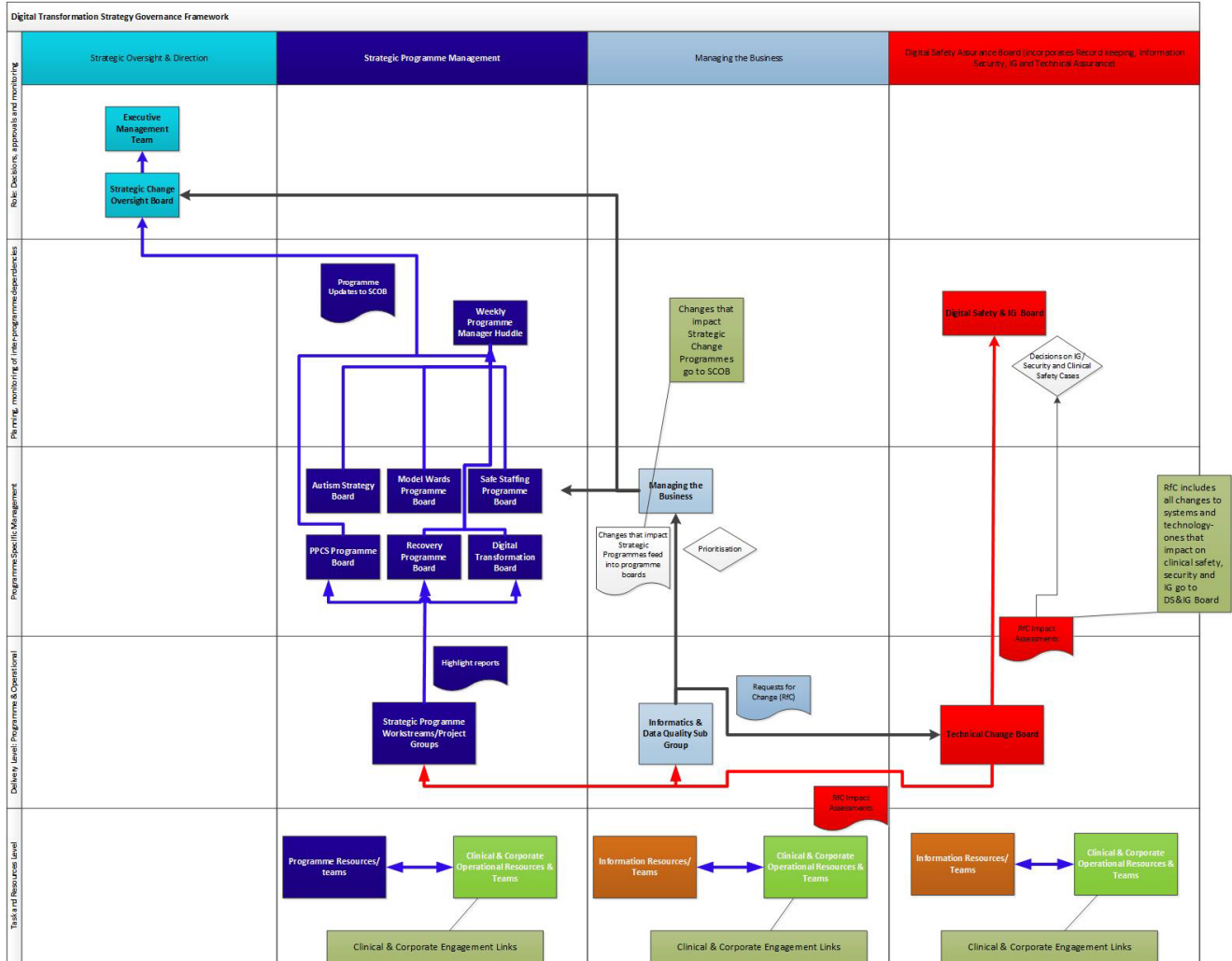
6 Document control

Date of approval:	01 August 2018	
Next review date:	31 May 2024	
This document replaces:	IT-0032-001-v2.1 Introduction or Upgrade of an Information System procedure	
Lead:	Name	Title
	Richard Yaldren	Head of Information Systems
Members of working party:	Name	Title
	GDPR steering group	
This document has been agreed and accepted by: (Director)	Name	Title
	Patrick McGahon	Director of Finance and Information
This document was approved by:	Name of committee/group	Date
	Digital Safety and Information Governance Board	01 August 2018
An equality analysis was completed on this document on:	31 July 2018	

Change record

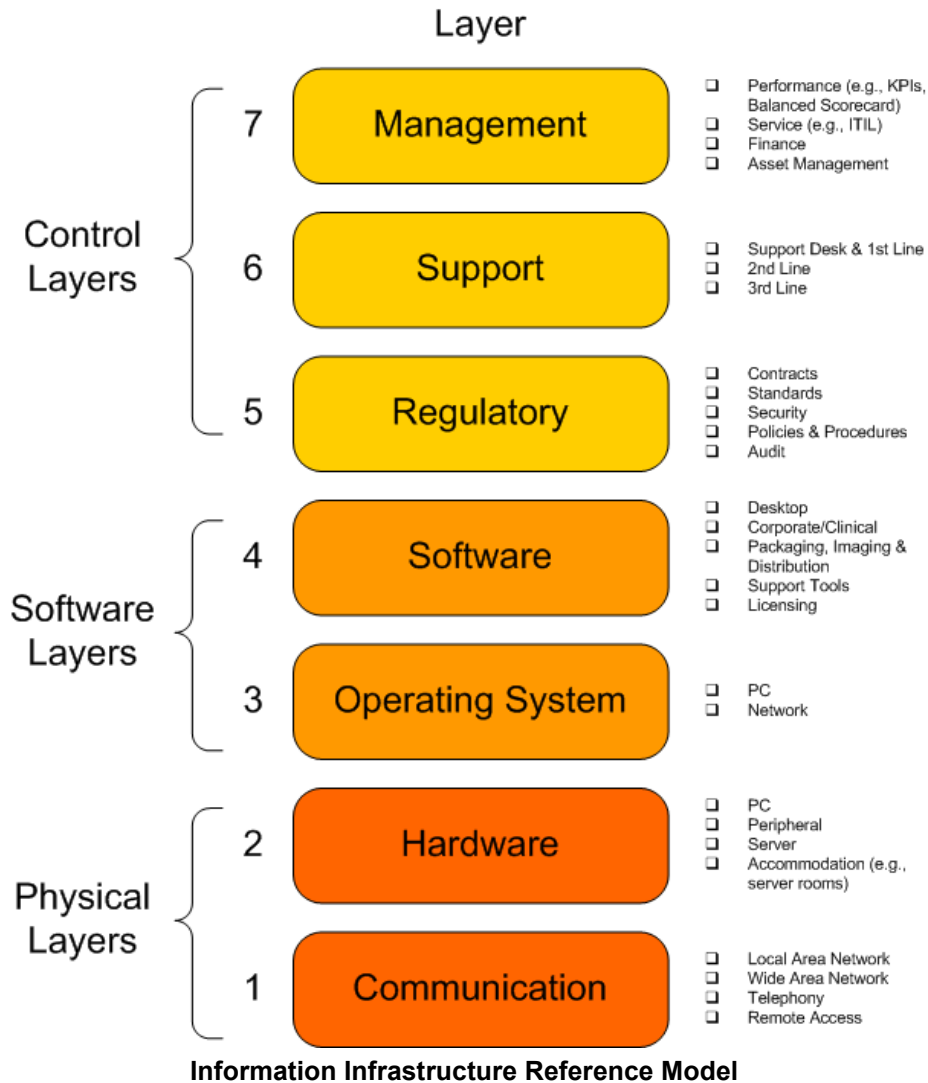
Version	Date	Amendment details	Status
2	April 2016	Renumbered from IT-0019-001 to IT-0032-001 to realign with the policy this procedure relates to	Withdrawn
2.2	Aug 2018	Reviewed in line with GDPR and current governance structure	Published
	Jul 2020	Review date extended 6 months	
	Jan 2022	Review date extended to 31 May 2022	
	Oct 2022	Review date extended to 31 May 2023	
2.2	Feb 2023	Review date extended to 31 May 2024	Published

Appendix 1: Process model for Form 0 to Form 3



Appendix 2 – OSI Seven-Layer Model

The Information Infrastructure Reference Model has been created to show all the areas of support required when running an information system.



The model enables the entire Information infrastructure for the trust to be represented using seven layers of detail. Each layer provides a separate level of abstraction and builds upon details presented in the layer beneath.

Layer 5 – Regulatory

The regulatory aspects of the IT infrastructure are located at this layer. The established rules for governing the supply and operation of components at layers 1 to 4 will include:

- Information governance
- Contracts and suppliers
- Software and hardware standards
- Security methods
- Policies and procedures
- Audit

Layer 6 – Support

The ways in which layers 1 to 5 are supported are located at the support layer. The support elements include:

- IM&T support desk and first line support
- Second line support
- Third line support

Layer 7 – Management

The management layer encompasses the processes and systems required to manage the entire Information infrastructure:

- IT service management (e.g., Information Technology Infrastructure Library, ISO 20000)
- Performance management (e.g., key performance indicators, balanced scorecard, service agreements)
- Budget management
- Project Management
- Asset Management

Layer Sets

The seven layers of the Information Infrastructure Reference Model separate into three sets:

1. the **physical layer set** comprises the *communication* and *hardware* layers (layers 1 and 2 respectively);
2. the **software layer set** comprises the *operating system* and *software* layers (layers 3 and 4 respectively);
3. the **control layer set** comprises the *regulatory*, *support*, and *management* layers (layers 5, 6, and 7 respectively).

Appendix 3 - Equality Analysis Screening Form

Please note; [The Equality Analysis Policy and Equality Analysis Guidance can be found on InTouch on the policies page](#)

Name of Service area, Directorate/Department i.e. substance misuse, corporate, finance etc.	Information Department, Finance and Information Directorate					
Name of responsible person and job title	Richard Yaldren, Head of Information Systems					
Name of working party, to include any other individuals, agencies or groups involved in this analysis	GDPR steering group					
Policy (document/service) name						
Is the area being assessed a...	Policy/Strategy	<input type="checkbox"/>	Service/Business plan	<input type="checkbox"/>	Project	<input type="checkbox"/>
	Procedure/Guidance			X	Code of practice	<input type="checkbox"/>
	Other – Please state					
Geographical area covered	Trust-wide					
Aims and objectives	Provide the principles that all information systems are implemented to					
Start date of Equality Analysis Screening	26 June 2018					
End date of Equality Analysis Screening	31 July 2018					

You must contact the EDHR team if you identify a negative impact. Please ring Sarah Jay or Ian Mhlanga on 0191 3336267/3046

1. Who does the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan benefit?					
The Trust will benefit by ensuring that information systems are implemented effectively. All new systems and upgrades to existing systems undergo due consideration of impacts on the information rights of individuals to ensure risks to information are understood and mitigated. This consideration will benefit patients, staff, carers and other individuals whose information is held and processed by the Trust.					
2. Will the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan impact negatively on any of the protected characteristic groups below?					
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 belief's)	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
<p>Yes – Please describe anticipated negative impact/s</p> <p>No – Please describe any positive impacts/s</p> <p>Each Trust system is considered individually to identify any potential negative impacts and the adjustments that can be made for individuals regarding accessibility and usability.</p>					

<p>3. Have you considered other sources of information such as; legislation, codes of practice, best practice, nice guidelines, CQC reports or feedback etc.? If 'No', why not?</p>	<p>Yes</p>	<p>X</p>	<p>No</p>	
<p>Sources of Information may include:</p> <ul style="list-style-type: none"> • Feedback from equality bodies, Care Quality Commission, Equality and Human Rights Commission, etc. • Investigation findings • Trust Strategic Direction • Data collection/analysis • National Guidance/Reports 	<ul style="list-style-type: none"> • Staff grievances • Media • Community Consultation/Consultation Groups • Internal Consultation • Research • Other (Please state below) <p>Data Protection Act 2018 (GDPR)</p>			
<p>4. Have you engaged or consulted with service users, carers, staff and other stakeholders including people from the following protected groups?: Race, Disability, Sex, Gender reassignment (Trans), Sexual Orientation (LGB), Religion or Belief, Age, Pregnancy and Maternity or Marriage and Civil Partnership</p>				
<p>Yes – Please describe the engagement and involvement that has taken place</p>				
<p>Yes – Workshops have been held throughout the Trust regarding GDPR and the new processes relating to this.</p>				
<p>No – Please describe future plans that you may have to engage and involve people from different groups</p>				
Empty space for 'No' response				

5. As part of this equality analysis have any training needs/service needs been identified?					
No	Please describe the identified training needs/service needs below				
A training need has been identified for;					
Trust staff	No	Service users	No	Contractors or other outside agencies	No
Make sure that you have checked the information and that you are comfortable that additional evidence can provided if you are required to do so					
The completed EA has been signed off by: You the Policy owner/manager: Type name: Richard Yaldren					Date: 01 Aug 2018
Your reporting (line) manager: Type name: Patrick McGahon					Date: 01 Aug 2018
If you need further advice or information on equality analysis, the EDHR team host surgeries to support you in this process, to book on and find out more please call: 0191 3336267/3046					



Tees, Esk and Wear Valleys
NHS Foundation Trust