Ashford and St. Peter's Hospitals
NHS Foundation Trust

Information Technology Change Policy

Authors: **Infrastructure Manager**

Executive Lead: **Simon Marshall, Director of Finance & Information**

Status: Approval date: October 2022

Ratified by: Information Governance Steering Group

Review date: October 2025

Patients first • Personal responsibility • Passion for excellence • Pride in our team

History

Issue	Date Issued	Brief Summary of Change	Author
1	October 2022	Initial Issue	Infrastructure Manager

For more information on the status of this document, please contact:	
Policy Author	Infrastructure Manager
Department/Directorate	Digital Services / Finance and Information
Date of issue	20 October 2022
Review due	20 October 2025
Ratified by	Information Governance Steering Group
Audience	All Digital Services Staff

Executive summary

This document is intended to provide a policy framework for changes to the Trust's Information Technology (IT) systems.

This framework covers IT changes to existing systems and small additions. Please use the Digital Technology Projects Policy for large or complex projects.

Contents

1. Introduction

This document is intended to provide a policy framework for all changes to Trust IT, including the following:

- Infrastructure applications
- Corporate systems
- Clinical systems, except for Surrey Safe Care which is covered by a separate Change Process. Please note, changes made under this policy may affect Surrey Safe Care.
- Other software
- End user devices
- Network equipment and configuration (switches, routers, firewalls etc)
- Other IT equipment, software, or configuration.

The aim of this policy is to ensure that all IT changes are carried out in a controlled and co-ordinated manner. It ensures that as far as possible everyone is made aware of changes that might affect their area of responsibility and ensures that all changes are done carefully to minimise any potential impacts.

The policy ensures that:

- Introduction of redundant changes that have the potential to disrupt services are minimised.
- Faults are not introduced during change implementation.
- All stakeholders are notified and consulted on a change.
- System owners are consulted of changes that may affect the systems they are responsible for.
- Only careful and considered risks are taken, in full knowledge of any dependencies.

2. Scope

This policy applies to all requestors and implementers of changes on Trust IT systems. Due to the current role-based access, it is expected that this includes:

- IT staff who may make a change, or request either they or another team member to make a change.
- Digital Services staff who request that IT make a change.
- Delivery partners or third-party providers who request or undertake a change.

This policy does not replace the Digital Technology Projects Policy used for complex projects requiring a great many alterations to systems, processes, or configurations. A Digital Initiative will likely cause several changes as described in this policy to be raised during implementation and having an approved initiative does not give permission to make IT changes.

As a condition of the enhanced privileges IT staff and 3rd Party Suppliers have (such as administrator rights on a machine or across a system), they are to abide by this Change Policy and ensure others do so.

This policy covers any Change Requests (CRs) related to:

- The Trust's IT Infrastructure, network, devices, and clinical systems, whether on premise or off premise.
- Changes made as part of a wider programme or project, such as Digital Initiatives.
- Cyber Security and Permission Changes

3. Purpose

The purpose of this policy is to ensure control over changes to the Trust's IT systems and technology, through the introduction of and adherence to standardised, repeatable change management processes.

4. Explanation of Terms Used

4.1. Change Management
Change management is an approach to moving organisations and their stakeholders, in an organized manner, from their current state to a desired future state.

4.2. Change Management Methodology
A system or approach which guides change implementers in performing a change.

4.3. Change Approval Board (CAB)
A meeting that decides whether a change can go ahead.

4.4. Gap Analysis
A process of assessing the current (as-is) state and the future (to-be) state in order to assess how to make the transition from one state to another.

4.5. Sponsor
A person or group which has the main interest in the process or result of a change initiative.

4.6. Outcome
The required result - a change of state from as-is to to-be, or a stage along the way. This may be as the results of a product being made available or a transformational change being completed.

4.7. Stakeholder
A person or group which has an interest in the process or result of a change initiative.

4.8. To-be state
The desired future situation in the organisation.

4.9. As-is state
This is the current situation in the organisation.

4.10 Baseline
The level of performance which is used for comparison after the change.

4.11 Change Initiative
An organised, concerted effort to alter part of or all of an organisation.

4.12. Digital Initiative

A project or programme, approved under the Digital Technology Projects Policy.

4.13. Information Technology Infrastructure Library (ITIL)

ITIL is an IT service management framework that outlines best practices for delivering IT services in a systematic and efficient way. This change process has been designed using the ITIL framework, adapted for our particular use.

5. Roles and Responsibilities

5.1. Trust Board

The Trust's Board is responsible for:

- ensuring there are appropriate policies and procedures in place that meet or exceed NHS requirements (nationally, regionally, and locally) and relevant laws and mandates, such as those set out within the Data Security and Protection (DSP) Toolkit.
- agreeing the Trust's risk appetite and risk management framework.
- acting as risk champions for the organisation, driving risk from the top down.
- ensuring all major decisions are subject to appropriate scrutiny, including risk assessment in line with the Trust's overarching Risk Management Framework.

5.2. Audit Committee

The Audit Committee is responsible for providing assurance to the Board on the adequacy and effective operation of internal systems of control and risk management across all the Trust.

5.3. Senior Information Risk Owner (SIRO)

The SIRO acts as an advocate for information risk on the board. The SIRO is expected to understand how the strategic business goals of the Trust generally, and IT specifically, may be impacted by information risks.

5.4. Head of Information Technology (IT)

The Head of IT is responsible for the development, implementation and embedding of this process with delegated authority from the SIRO.

The Head of IT is also responsible for:

- The management of risk within the IT department
- Approval of expenditure at values defined with the Trust's Standing Financial Instructions (SFIs)
- Ensuring IT staff are empowered and trained to identify, report, and manage risks within their area of responsibility or team
- The potential transfer of risk(s) between departments and/or other directorates where risks are transferrable
- Development of local risk registers and their maintenance, through delegation via the IT management structure
- Monitoring and reviewing of departmental risk registers within agreed local forums/groups

- The escalation of risks that cannot be managed locally or that pose a threat to Trust objectives
- Ensuring that the department's approach to information risk is effective in terms of resource, commitment, and execution and that this is communicated to all staff.

5.5. Infrastructure Manager

The Infrastructure Manager is responsible for the routine running and application of the Change process. They will lead Change Approval Board and ensure the process is followed correctly.

5.6. IT Department

All IT department staff are responsible for ensuring that they read, understand, and abide by this Policy and the associated IT procedure.

5.7. Information Asset Owners (IAO)

IAOs are responsible for ensuring that a DPIA is in place when implementing a change or a new process. Any additions or alterations can be completed through the Information governance team.
IAOs are also responsible for making sure that changes are handled in accordance with this policy.

5.8. Change Initiator

Responsible for providing the information to the Change process, this could be the Project Manager or IAO.

5.9. Change Owner

Responsible for carrying out the change in accordance with this policy and any conditions from the Change Approval Board.

6. Policy

6.1. Definition of a Change

ITIL defines a Change as:

The addition, modification, or removal of any authorised, planned, or supported service or service component that could have an effect on IT services.

6.2. Types of Changes

A change request can be initiated by any of the following:
- A member of the IT Department
- An end user, including IAOs
- A supplier
- A project output

- Any other department in Digital Services

6.2.1. Standard Changes

A standard change is a low-risk change, that follows a defined and standard process. Examples of this could be:

- Additional firewall rules.
- New virtual machine.
- New admin accounts.

Standard changes are listed as Service Requests in Hornbill, the Trust IT Service Management System, these can be added to as needed by the Hornbill administration team. An approver can still be used with this workflow if desired, but standard changes will not be discussed at CAB and do not have to wait for CAB approval to proceed.

Standard changes should not generally have any perceived impact to users or services.

6.2.2. Normal Changes

A normal change includes most changes and includes everything not captured under a Standard or Emergency change.
Most changes fit into this category, examples of this could be:

- Changes needed to support an approved Digital Initiative.
- Changes to core networking such as VLANs, internet, failover testing, etc.
- Changes to security settings and posture.
- Changes to existing in service applications.

6.2.3. Emergency Changes

An emergency change is a change that must happen imminently and cannot be planned for.

It should be noted, an urgent change is not an emergency change – an emergency change must result from an event beyond our control, not urgency or lack of planning on our or a supplier's part.

Examples of this could be:

- Emerging cyber threat or alert.
- Workaround for a problem that is disrupting service.

Where possible, verbal approval from key stakeholders should be gained before carrying out an emergency change. It is understood this cannot always take place when on call, for instance.

An emergency change must have a retrospective change request submitted by the normal process, which will be reviewed at the next CAB.

6.2.4. Major Changes

A Major Change is a complex, high risk, and high impact change, it may include a phased programme of standard changes to reduce the overall risk.

Due to the risk and impact involved, Major Changes will be evaluated carefully, and care should be taken presented with plans to reduce risks & impacts where possible.

Examples of this could be:

- Replacement of the Trust's Server Infrastructure.
- Firewall replacement.
- Replacement of a clinical system.

6.3. Business Continuity Risk Assessment

Changes that will or may cause an impact to the normal running of Trust business will require a Business Continuity Risk Assessment (BCRA). This includes any change where users will need to implement their Business Continuity procedures.

Guidance for completing BCRA can be found on TrustNet in the Business Continuity Plan Policy.

6.4. Normal Change Request Process

6.4.1. A Service Request is Raised on Hornbill

Follow the Hornbill workflow which will guide you through the process. If there is an approval pending in Hornbill, you may not proceed with the change until this is approved.

Service owners are responsible for approving requests (if required) within their own area of responsibility, where further information is required, this should be sought.

Many service requests are open for all Trust staff, some are limited to Digital Services only. If the Change Owner does not believe a change should proceed, they should seek advice from the Infrastructure Manager, the CAB, or other appropriate person.

6.4.2. Change is Considered by the CAB

The Change Initiator and Change Owner should present the Change, highlighting the benefits of the change, along with any risks and issues.

6.4.3. Change is Implemented

If approved, the Change Owner should implement the change at the planned time, and resolve the call once completed. Any conditions the CAB request must be adhered to.

If rejected, the Change Owner must not implement the change.

If a change is delayed, the Infrastructure Manager must be informed.

7. Training

Training is not expected to be needed for most staff to undertake their roles and responsibilities as defined in this policy and associated process.

If you are unsure how to proceed, contact Asp-tr.ITChanges@nhs.net or a member of IT who can help you.