



**Business Continuity, Disaster Recovery and Backup in Relation to I.T.**

Version	3.3
Designation of Policy Author(s)	Head of Information Governance and Patient Records
Policy Development Contributor(s)	Head of Technology
Designation of Sponsor	Chief Information Officer
Responsible Committee	Information Governance Committee
Date ratified	14/02/2023
Date Issued	01/04/2024
Review date	31/03/2025
Coverage	Trust Wide

The Trust is committed to a duty of candour by ensuring that all interactions with patients, relatives, carers, the general public, commissioners, governors, staff and regulators are honest, open, transparent and appropriate and conducted in a timely manner. These interactions be they verbal, written or electronic will be conducted in line with the NPSA, 'Being Open' alert, (NPSA/2009/PSA003 available at [www.nrls.npsa.nhs.uk/beingopen](http://www.nrls.npsa.nhs.uk/beingopen) and other relevant regulatory standards and prevailing legislation and NHS constitution)

It is essential in communications with patients that when mistakes are made and/or patients have a poor experience that this is explained in a plain language manner making a clear apology for any harm or distress caused.

The Trust will monitor compliance with the principles of both the duty of candour and being open NPSA alert through analysis of claims, complaints and serious untoward incidents recorded within the Ulysses Risk Management System.

<b>1</b>	<b>Executive Summary</b> .....	<b>3</b>
	Applicability and Scope.....	3
<b>2</b>	<b>Introduction</b> .....	<b>3</b>
<b>3</b>	<b>Policy Objectives</b> .....	<b>3</b>
<b>4</b>	<b>Duties and Responsibilities</b> .....	<b>3</b>
<b>5</b>	<b>Main Provisions</b> .....	<b>4</b>
	5.1 General Provisions .....	4
	5.2 Business Continuity Plan .....	4
	5.3 Frequency and Timings of Back Up of the Trust Network	
	5.4 Backup Retention Policy.....	5
	5.5 Backup Failure .....	6
	5.6 Restores.....	6
<b>6</b>	<b>Key References</b> .....	<b>7</b>
<b>7</b>	<b>Associated Documents</b> .....	<b>7</b>
<b>8</b>	<b>Training</b> .....	<b>7</b>
<b>9</b>	<b>Policy Administration</b> .....	<b>7</b>
<b>10</b>	<b>Consultation, Communication and Implementation</b> .....	<b>7</b>
<b>11</b>	<b>Monitoring Compliance with the Policy</b> .....	Error! Bookmark not defined.
<b>12</b>	<b>Performance Management of the Policy</b> .....	Error! Bookmark not defined.
<b>13</b>	<b>Initial Equality Impact Assessment Screening Tool</b> .....	<b>9</b>

## 1 Executive Summary

### Applicability and Scope

- i. This policy covers all aspects of information within the organisation, including (but not limited to) patient/client/service user information, personnel information, organisational information
- ii. This Policy covers all aspects of handling information within the organisation, including (but not limited to) structured record systems (paper and electronic) and transmission of information
- iii. This Policy covers all Information systems purchased, developed and managed by/on behalf of, the organisation and any individual directly employed or any individual undertaking activity under the control or direction of the organisation.

## 2 Introduction

- i. The Trust regards all person identifiable information that it holds or processes as confidential and will implement and maintain policies to ensure compliance with all necessary mandatory obligations
- ii. The Trust recognises the importance of reliable information, both in terms of the clinical management of individual patients and the efficient management of services and resources. Effective information governance plays a key part in supporting clinical governance, service planning and performance management
- iii. Effective Information Governance gives assurance to the Trust and to individuals that personal information is dealt with legally, securely, efficiently, and effectively to deliver the best possible care.
- iv. The Trust will ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management

## 3 Policy Objectives

- i. To define the standards and Trust rules for all individuals for Business Continuity, Disaster Recovery and Backup

## 4 Duties and Responsibilities

- 4.1 The Senior Information Risk Owner
  - Is accountable for Information Governance and Information Security at a Trust level, which includes the risk assessment process for information risk, including review of annual information risk assessments that support and inform the Statement of Internal Control.
  - Reviews and approve actions in respect of identified information risks
  - Ensures that the organisation's approach to information risk is effective in terms of resource, commitment, and execution
  - Sets the overall objectives for Information Security for the Trust

#### 4.2 Caldicott Guardian

- Is agreed as the 'conscience' of the organisation and to advise the Trust Board on matters relating to confidentiality.
- Reviews and approves protocols governing the disclosure of patient information across organisational boundaries.
- Approves the release of information where consent from the data subject is not considered necessary or appropriate

#### 4.3 Chief Information Officer

- Has overall responsibility for Information Security for the Trust
- Ensures the overall approach taken to managing Information Security, Information Systems and Information technology is appropriate

#### 4.4 Head of Technology

- Is responsible for the management of Information Security across the Trust.
- Monitors local responses to Information Security incidents and provide support in developing proportionate and effective responses to manage risk.
- To be responsible, as operational Lead, for IT services and the associated security risks.
- Manages the Trust Information Technology infrastructure on a day to day basis as directed by the Chief Information Officer

## 5 Main Provisions

### 5.1 General Provisions

- The Head of Technology will ensure that, where Business Continuity plans are necessary, they will align with relevant Disaster Recovery and Backup plans.
- The Head of Technology will ensure that due account is taken of the Trust overall Business Continuity and Disaster Recovery Plans when implementing IT related Business Continuity, Disaster Recovery and Backup Plans.

### 5.2 Business Continuity Plan

- The Head of Technology will maintain an effective and up to date Business Continuity Plan that will define actions to be taken if an event occurs that requires the plan to be implemented.
- The Business Continuity Plan will include:
  - Identification of all responsibilities and emergency procedures
  - The procedures to be followed to ensure the plans operate effectively and within the required timescales.
  - The agreed procedures and processes
  - How the Business Continuity Plan will be tested and verified as effective
  - The resources needed to enable the Business Continuity Plan to operate effectively

- iii. The Business Continuity Plan will be unambiguous and in sufficient details to ensure there are no doubts as to what is needed to put such a plan into practice
- iv. The Business Continuity Plan will clearly specify the conditions under which it will be activated, as well as details of the individuals responsible for executing each component of the plan.
- v. The Head of Technology will ensure that an up-to-date risk register is maintained and each risk on the register is appropriately managed.
- vi. The Head of Technology will ensure that, so far as is reasonably practical:
  - All necessary plans are in place to maximise preparedness
  - Preparation is such that Trust may be assured that risks are managed, contingencies are in place, contingencies will be implemented in the event that implementation is needed, and contingencies will be effective.
- vii. The Head of Technology will ensure that Business Continuity Plans are tested:
  - At least annually
  - Whenever there is a significant change to the plan itself
  - Whenever there is an incident that caused the plan to be implemented
- viii. The Head of Technology will maintain an annual rolling programme of testing of the Trust Information Technology infrastructure so that it is sufficiently protected by Business Continuity Plans, Disaster Recovery Plans and Backup regimes and will ensure the programme is implemented

### **5.3 Frequency and Timings of Back Up of the Trust Network**

- i. Systems and data hosted on core infrastructure within the Trust core data centres will be backed up according to the following regime:
  - A backup will be undertaken daily 7 days per week, 365 days per year
  - Daily backups will be supplemented with an incremental backup and/or snapshots where the hardware has this functionality
  - Ad-hoc backups will be performed as requested or required

### **5.4 Backup Retention Policy**

- i. Systems and data hosted on core infrastructure within the Trust core data centres will be retained in accordance with the relevant technical Appendix
- ii. External or 3<sup>rd</sup> party systems that are used to support the delivery of services to patients, visitors and employees of the Trust will be retained in accordance with agreements that are reached with each third-party provider

## 5.5 Backup Failure

- i. The Head of Technology will ensure that effective processes are in place to respond appropriately to a failure of backup of systems and data hosted on core infrastructure within the Trust core data centre.
- ii. The Head of Technology will ensure that there are clear responsibilities and business arrangements between the Trust and any 3<sup>rd</sup> party system suppliers and such arrangements state clearly that the responsibility to resolve issues, and inform systems owners, rests with the 3<sup>rd</sup> party supplier

## 5.6 Restores

- i. The Head of Technology will ensure that appropriate arrangements are in place to ensure that planned validation and testing of backup of data is undertaken on a quarterly basis, supplemented by ad-hoc restores and testing as and when required
- ii. The Head of Technology will ensure that there are clear responsibilities and business arrangements between the Trust and any 3<sup>rd</sup> party suppliers, and such arrangements will state clearly that the responsibility for restoration and associated validation rests with the 3<sup>rd</sup> party supplier.

## 5.7 Authority to Act

- i. Approving Officers are, for the purposes of this Policy:
  - Chief Information Officer
  - Head of Technology
  - IT Operations Manager
- ii. Authority to vary from this policy for a specific reason and a time limited period can be given by an Approving Officer
- iii. An Approving Officer shall not be allowed to give authority where giving such authority would give rise to a conflict of interest
- iv. Authority to vary from this Policy, which is not time-limited, may initially be given by an Approving Officer but this must then be approved by the Information Governance Committee at the first opportunity

## 5.8 Reporting

- i. The Information Governance Committee shall be informed of any incidents where the cause is a systematic failure of any of its systems of control
- ii. All Managers will provide reasonable access to any system, area or individual that will allow the Information Governance Department to assess compliance to this policy through the Spot-check Programme

## 6 Key References

- i. The Data Protection Act 2018
- ii. The General Data Protection Regulations
- iii. The Information Security NHS Code of Practice
- iv. The NHS Confidentiality Code of Practice
- v. The Records Management NHS Code of Practice
- vi. Freedom of Information Act 2000
- vii. Data Security and Protection Toolkit
- viii. The Computer Misuse Act

## 7 Associated Documents

None

## 8 Training

- i. Training for implementation of this policy is contained within the Trust overall training program and is reference by the Information Governance and Information Security Policy and Framework

## 9 Policy Administration

## 10 Consultation, Communication and Implementation

Consultation Required	Authorised By	Date Authorised	Comments
Impact Assessment			
GDPR	R Cowell	14/02/2023	None
Have the relevant details of the 2010 Bribery Act been considered in the drafting of this policy to minimise as far as reasonably practicable the potential for bribery?	Yes		
External Stakeholders			
Trust Staff Consultation via Intranet	Start date: February 2023		End Date: February 2023
Describe the Implementation Plan for the Policy (and guideline if impacts upon policy) (Considerations include; launch event, awareness sessions, communication / training via CBU's and other management structures, etc)			By Whom will this be Delivered?
The policy is existence already			

### Version History

Date	Version	Author Name and Designation	Summary of Main Changes
21/08/2017	1.0	Russell Cowell, Head of Information Governance	Policy has been completely reviewed and re-written. Policy version set to version 1.0 to reflect the substantial changes and the fact that it has been developed as an integrated policy set
03/03/2018	1.1	Russell Cowell, Head of Information Governance	Periodic review. Minimal updates to wording and KPIs. Addition of IT Operations Manager as a 'Approving Officer'
06/01/2020	2.0	Russell Cowell, Head of Information Governance	Major review and revision of wording considering lessons learned, introduction of new governance arrangements, insertion of GDPR definitions and provisions following independent external review by Data Protection Officer
04/12/2020	3.0	Russell Cowell, Head of Information Governance	General review and minor update on policy wording to make provisions clearer based on experience. Enhancements to provisions on cyber security, re-organisation of paragraphs within policies (without word changing) so some text now moved into other policies and vice versa
31/03/2022	3.1	Russel Cowell, Head of Information Governance	Review only and re-approval. No changes
31/03/2023	3.2	Russell Cowell, Head of Information Governance and Records	General wording review and re-approval by Information Governance Committee. Update to job title of Head of Information Governance to add "and Records" to title. Re-allocation of policy sponsorship to the Chief Information Officer
31/03/2024	3.3	Russell Cowell, Head of Information Governance and Patient Records	General review and re-approval. No significant changes.



# 11 Equality Impact Assessment

<b>Does The Policy Affect:</b>	<b>Staff</b>		<b>Patients</b>		<b>Both</b>	<b>X</b>
--------------------------------	--------------	--	-----------------	--	-------------	----------

<b>Equality Group</b>	<b>Impact (Positive/Negative/Neutral)</b>
<b>Race</b> (All Ethnic Group)	Neutral
<b>Disability</b> (Inc Physical, long term health conditions & Mental Impairments)	Neutral
<b>Sex</b>	Neutral
<b>Gender Re-Assignment</b>	Neutral
<b>Religion Or Belief</b>	Neutral
<b>Sexual Orientation</b>	Neutral
<b>Age</b>	Neutral
<b>Marriage &amp; Civil Partnership</b>	Neutral
<b>Pregnancy &amp; Maternity</b>	Neutral
<b>Other</b> e.g., caring responsibilities, human rights etc.	Neutral

**For each protected characteristic, consider whether the impact is positive. If so, provide supporting evidence to demonstrate how your decision was made and the impact that the policy will have with consideration of each protected characteristic (e.g., protected characteristic – impact – rationale)**

Not Applicable

**For each protected characteristic, consider whether the impact is negative. If so, provide supporting evidence to demonstrate how your decision was made and the impact that the policy will have with consideration of each protected characteristic (e.g., protected characteristic – impact – rationale)**

Not Applicable

**If your assessment has identified any negative impacts, please detail any actions that have been put in place to mitigate these (upon approval of EIA these actions will be shared with the Equality, Diversity and Inclusion Committee):**

<b>Outcome</b>	<b>Actions Required</b>	<b>Time Scale</b>	<b>Responsible Officer</b>

**Is there evidence that the s. 149 Public Sector Equality Duties (PSEDs) will be met? Consider whether the proposed policy will...**

- Eliminate discrimination, victimisation, harassment, and any unlawful conduct that is prohibited under this act
- Advance Equality of opportunity
- Remove or minimise disadvantages suffered by people who share a relevant protected characteristic that are connected to that characteristic
- Take steps to meet the needs of people who share a relevant protected characteristic that are different from the needs of people who do not share it
- Encourage people who share a relevant protected characteristic to participate in public life or in any other activity in which participation by such people is disproportionately low.
- Foster good relations between persons who share a relevant protected characteristic and persons who do not share it. (Consider whether this is engaged. If engaged, consider how the project tackles prejudice and promotes understanding - between the protected characteristics)

**Explain your answers below.**

The policy is an administrative policy, which implements established legal obligations neutrally.

**Does the EIA have regard to the need to reduce inequalities for patients with access to health services and the outcomes achieved? (this section is a requirement for any services outlined within the NHS England and Improvement [Core 20 Plus 5](#) approach to health inequalities) Explain.**

The policy is an administrative policy, which implements established legal obligations neutrally.

**Section 2:**

**To be completed by the EDI Manager authorising the EIA**

**Anything for noting or any recommendations for consideration by the Board**

*Guidance Note: Will PSEDs be met? Are Core 20 Plus 5 services considering patient health inequalities?*

**Review Date:**

**Additional Supporting Evidence and Comments:**