**Policy**

2014

**Information Technology Management**

**Ian Mellors, Andrew Taylor, Julia Taylor, Andrew Bright, John Clinton,**

**Information Technology Management**

|  |  |
| --- | --- |
| **Effective From:** | Full date 23/12/2014 |
| **Expiry Date:**  | Full date 23/12/2016 |
| **Date Ratified:**  | Full date 23/12/2014 |
| **Ratified by:**  | Laboratory Medicine Clinical Governance and Quality Committee |

#### Contents

1. **Introduction**
2. **Scope**
3. **Aim**
4. **Roles and Responsibilities**
5. **Definitions**
6. **Policy**
7. **Training**
8. **Policy Compliance Monitoring**
9. **Related Documents**
10. **Consultation and Review**
11. **Implementing**
12. **References**
13. **Associated documentation**
14. **Introduction**

Information Technology (IT) systems are crucially important in the day to day business of the Directorate of Laboratory Medicine and that of the individual departments that operate within it. Many of the systems are critical to the operation of equipment, administrative systems, communication, end user connectivity and intermeshing with the IT systems and strategies of the parent organisation (NUTH) and beyond. There needs to be a clear mapping of the entire IT connectivity with clearly defined roles and expectations of practitioners at all stages of the IT connectivity processes. This is particularly prevalent when IT systems fail and recovery actions are required. The expectations of practitioners involved in all parts of recovery processes and the intermeshing of activities and timescales are particularly important and this policy is intended to state the position of the Directorate of Laboratory Medicine and the departments under its auspice. Minor disruptions to service may be managed locally or with input from the NUTH IT helpdesk but significant service loss will require a broader scope and direct appropriate management of the situation.

The roles and responsibilities/accountabilities of all internal and externally contracted parties must be defined and the performance requirements of key individuals acting on their behalves must be stated. The general organisational recovery timeframes for each party plus the chain sequence of events for disaster recovery must be documented. These are added in general terms to this policy.

The Directorate of Laboratory Medicine, through the Trust, must ensure the highest possible level of service to patients and this must be maintained irrespective of what occurs to the infrastructure, communications and facilities. There is a need to prioritise and allocate resources appropriately when faced with adverse situations and ensure that appropriate management applies at all times. This should be underpinned by risk assessment and contingency planning where possible.

1. **Policy Scope**

This policy defines the Directorate of Laboratory Medicine management requirements for the management of its information technology (IT) systems. It describes the intermeshing with parent organisation (NUTH) IT systems and details the roles, responsibilities and accountabilities of all members of staff in the IT governance chain (from individual users through to IT leads within NUTH). It is crucial to the business continuity that failure risks associated with the IT systems used are identified and that recovery plans are formulated and tested regularly for continued effectiveness. The policy is linked to the Directorate business continuity plan and the Trust Business Continuity Policy

Although not exhaustive, the scope of the policy covers the following IT risk categories:

1. Server loss due to fire or other physical damage (local and/or central NUTH IT)
2. Air conditioning failure
3. Hardware failure (local or central NUTH)
4. Software failure (local or central NUTH)
5. Loss of data
6. Theft
7. Fraud
8. Internet access to external sites
9. Network disruption (to entire organisation, NHS, or local)
10. Loss of email service
11. Loss of directory services
12. Malware
13. Loss of key staff
14. Loss of middleware and/or connectivity
15. Power supply to systems and/or parent organisation
16. Loss of external network
17. Loss of business
18. Damage to reputation
19. Risk to patient welfare
20. Malware including hacking and spyware

To ensure that a robust IT service is provided, it is necessary to ensure that all appropriate IT training and induction occurs and that this is tested by scheduled regular competency assessment for all grades of user.

The policy applies to all staff grades within The Directorate of Laboratory Medicine and also to personnel who provide diagnostic support services in areas that operate under the auspice of The Directorate of Laboratory Medicine.

**This policy should be used in conjunction with the current NUTH Business Continuity policy**

1. **Aims of Policy**

The aims of the policy are to ensure that:

* + 1. All IT incidents, accidents, nonconformities and non-compliances occurring within the Directorate of Laboratory Medicine and its departments are recorded, processed, escalated appropriately with timely and effective corrective and remedial actions formulated and introduced. All incidents are to be fully investigated with root cause being determined, action plans devised and all corrective measures taken being tested for effectiveness.
		2. The roles and responsibilities of all practitioners, in the entire IT connectivity chain, are defined and understood.
		3. Channels of communication for IT systems recovery are defined and that the interrelationships with the parent organisation are fully understood with defined areas of responsibilities and accountabilities.
		4. Recovery strategies are understood and have been tested for effectiveness (audit).
		5. There is business continuity in the event of IT system failure.
		6. There is minimum disruption to services.
		7. There is minimum impact on reputation.
		8. Appropriate escalation processes are in place dependant on incident severity.
1. **Duties – Roles and Responsibilities**
	* 1. **Trust Board -** The Trust Board is responsible for implementing a robust system of corporate governance within the organisation. This includes having a systematic process for the development, management and authorisation of strategies, policies and procedures and the Chief Executive is ultimately responsible for ensuring effective corporate governance within the organisation.
		2. **Chief Executive -** The Chief Executive has overall responsibility for Business Continuity, on behalf of the Board of Directors of the Trust. The Chief Executive is responsible for ensuring that the Trust is in a position to provide an overall assurance that the organisation has in place the necessary Business Continuity Framework.
		3. **Executive Lead for Business Continuity -** The Executive Lead for Business Continuity has delegated responsibility for ensuring that the Trust is in a position to provide assurance that the organisation has in place the necessary Business Continuity Framework and is also a member of the Trust Board subcommittee, the Business Continuity Steering Group.
		4. **Lead Manager for Business Continuity**

The Lead Manager for Business Continuity in the Trust is responsible for:-

1. Leading the planning and implementation of the Trust’s Business Continuity Management Framework and System.

1. Developing and maintaining the Business Continuity Policy, plan and process.
2. Supporting directorates and departments with their Business Continuity responsibilities.
3. Ensuring there is appropriate alignment of directorates’ and departments’ individual Business Impact Assessments and Business Continuity Plans with corporate objectives.
4. Co-ordinating the production of necessary Trust or site wide Business Continuity Plans.
5. Implementing and maintaining a system for central storage and retrieval of Trust Business Continuity Plans.
6. Undertaking consistency checking of plans
7. Leading evaluation of incidents and identifying organisational learning points.
	* 1. **Directorate and departmental managers**

Directorate and departmental managers are responsible for leading and implementing the Business Continuity process for all areas within their control.

They should ensure that:-

1. The Laboratory Manager for each department is the designated business continuity lead/s for their area of responsibility.

1. Business Impact Analysis of services is undertaken/reviewed at least annually as part of each individual department annual management review.

1. Business Cases and implementation plans for new IT systems should specifically address Business Continuity arrangements.

1. Business Impact Assessment and where appropriate Business Continuity planning should be undertaken ideally prior to or as soon as possible after any material changes to a directorate/department’s management or organisational structure/ service portfolio or location of services.

1. Business Continuity Plans for new services should be reviewed after the first six months of service operation.
2. Business Impact Assessment is undertaken and recovery requirements and down time plans are developed for new IT systems, prior to implementation.

1. A Business Continuity Strategy is agreed and documented in response to identified risks.

1. Threats and risks which have the potential to disrupt the smooth running of services are regularly considered and reviewed and that, where economically appropriate, systems and processes are made sufficiently robust and resilient to withstand these threats.
2. Business Continuity Plans are developed and implemented for key services to meet the agreed recovery time requirements in Business Impact Assessments.

1. Business Continuity Plans are reviewed and updated as required at least annually and those plans are used to minimise the effects of business continuity incidents. The Laboratory Medicine IT Manager is responsible for this action and the Clinical Director of Laboratory Medicine is the ultimate approver

1. Joint planning is undertaken where services overlap with other directorates /departments or have key inter-dependencies.

1. Documented Business Continuity Plans for key services, in particular those with a Recovery Time Objective of no more than 24 hours, are tested for effectiveness on at least an annual basis.

1. Staff essential to recovery of services are identified and can be contacted during an emergency. Laboratory Managers are responsible for ensuring that current and valid contact lists are available within the departments and that staff have access to these. Laboratory Managers may delegate responsibility for list update. Individual department business continuity plans will include personnel to be contacted and personnel should refer to the appropriate contact list for their areas of work.

1. The contents of the directorate/department Business Continuity Plans and invocation procedures are communicated to relevant staff at a minimum annually.

1. Specifically documented directorate/department down time plans for IT is tested biannually at a minimum. This should be part of a scheduled program of audit.

1. Business Continuity Plans are stored in sufficient alternative locations and formats (paper and electronically) to ensure availability in a Business Continuity incident.
2. Staff are enabled to attend training to support the effective implementation of the Business Continuity Policy according to the needs of their specific roles and responsibilities in the Business Continuity Planning process.
	* 1. **Laboratory Medicine IT Manager –** is responsible for ensuring the functionality and maintenance of the Laboratory Medicine Information systems including software updates, help facilities for the information system, managing storage and retrieval of records and ensuring that all operational and instructional documentation is current and valid. The IT Manager is responsible for ensuring regular end to end testing occurs and that this is subjected to planned schedules of audit, with records of compliance held. The IT Manager will also ensure that nonconformities and complaints are fully investigated with root causes identified where possible and corrective and remedial actions implemented as appropriate. The Laboratory Medicine IT Manager is responsible for ensuring full verification of manufacturer validation is undertaken before the introduction of any modifications and changes that can impact on test results. The Laboratory Medicine IT Manager is responsible for producing and maintaining the directorate plan to recover from IT failure.

* + 1. **Laboratory Manager –** will ensure that systems are in place to ensure continued IT suitability and functionality in their areas of responsibility and for the continuation of services in the event of IT failure. They are responsible for ensuring that business continuity plans are current, valid and have been tested regularly for effectiveness (at least every 2 years).
		2. **Laboratory Operational Managers -** are responsible for ensuring the continuation of services in the event of an IT systems failure and dependent upon the severity, to manage the impact upon the services provided and the reputation of the department/directorate. They will coordinate activities within their department and liaise with department IT leads to determine functionality status and will delegate resources as appropriate in response.
		3. **Department IT Leads –** are the first point of contact for IT issues in individual laboratories. They will liaise directly with the Laboratory Medicine IT Manager and with individual Laboratory Managers as appropriate regarding IT functionality and issues. The IT leads will provide limited cross department/discipline cover as required to ensure continued IT functionality.
		4. **All Staff Members -** All members of staff must comply with the conditions contained within this document and assist in recovery of services as directed by laboratory management. Staff in training must be supervised by a competent member of staff. All staff members will be expected to access patient data and information relevant to the task in hand, including entering patient details and examination results, making appropriate changes and authorising the release of results and reports (dependant on grade and levels of training, knowledge and experience).
1. **Definitions**
	1. **Policy**
		1. A policy enables management and staff to make correct decisions, deal effectively with and comply with relevant legislation, guidelines and organisational rules and practices.
	2. **Procedure**
		1. This is a set of detailed step by step instructions that describe the appropriate method for carrying out tasks or activities.
	3. **Protocols**
		1. Protocols are rigid statements allowing little or no flexibility or variation. A protocol sets out a precise sequence of activities to be adhered to in the management of a specific clinical condition.
	4. **Guidelines**
		1. These are systemically developed statements that assist in making decisions
	5. **Strategy**
		1. This is a plan of action designed to achieve a long-term or overall aim.
	6. **Competence**
		1. The extent of someone’s or something’s ability.
	7. **Information Technology**
		1. A term commonly used as a synonym for computers and computer networks but it also applies to other distribution networks e.g. telephones.
2. **Policy**

**Laboratory Medicine - IT interactions**

* + 1. The IT interrelations within Laboratory Medicine and NUTH can be generally represented as follows:

**Interrelationships and Connectivity within IT**

* + 1. The IT interrelations within Laboratory Medicine are represented as follows:

Key

 IT Interaction Lines

 Management Lines

**NUTH IT**

**Laboratory Medicine Executive**

**Clinical Director Laboratory Medicine**

**Laboratory Medicine IT Manager**

**Microbiology & PHE**

 **Laboratory Manager**

**Cellular Pathology**

**Laboratory Manager**

**Blood Sciences**

**Laboratory Manager**

**Microbiology & PHE**

 **IT Lead**

**Cellular Pathology**

**IT Lead**

**Blood Sciences**

**IT Lead**

**Microbiology and PHE Laboratory Section Leads**

**Cellular Pathology Laboratory Section Leads**

**Blood Sciences Laboratory Section Leads**

* + 1. Each department within Laboratory Medicine (Blood Sciences, Cellular Pathology and Microbiology/Public Health England [PHE]) has designated IT leads that are the contact point for all IT issues that originate within each laboratory. The section leads within each department are responsible for feeding IT issues to the IT department Leads who in turn feed into the Laboratory Medicine IT Manager or deputy IT Manager. Escalation and management of an IT issue is dependent on the severity and the department IT leads will determine whether it can be managed locally or requires higher level input in the IT chain.
		2. The Clinical Director of Laboratory Medicine (or deputy) and the Laboratory Manager for each department within the directorate (or deputy), will be informed of all major incidents that impact on the service and they will instigate appropriate management actions in line with the NUTH Business Continuity policy.
		3. The responses to an IT incident will be measured and will reflect the severity of the incident. The general rule of thumb is that small, routine and non-urgent IT issues should be escalated through the various Laboratory Department IT leads and the more critical impacts are likely to come from the Trust downward and will require management through the NUTH ‘Business Management Continuity Policy’. Non-urgent requirements will be addressed as soon as practicably possible and will be prioritised according to need and impact. The major incidents will be managed within time frames indicated in the ***‘IT and Communications Applications and Data Recovery Requirements’*** section of this policy (3.1.36, 3.1.37, and 3.1.38).
		4. The Clinical Director for Laboratory Medicine will ensure that all incidents are investigated and appropriate responses are implemented and will delegate appropriate responsibilities for this dependent on the severity. Although not exhaustive, this includes the following groups in Laboratory Medicine:
1. Clinical Leads
2. Laboratory Managers
3. Laboratory Medicine Quality and Governance Committee
4. Department Quality and Governance Committees
5. Laboratory Medicine IT Manager

The committees and individuals above may delegate responsibilities for investigation as required and within agreed achievable investigative timeframes

**Information System Management**

* + 1. The Laboratory Medicine IT Manager has overall responsibility for the continued smooth running of Laboratory Medicine IT systems and for ensuring that all necessary systems are in place to maintain services. They may delegate individual tasks to Laboratory Medicine department IT leads or deputies but they retain overall accountability for continued service. They will act as the conduit for Trust and Laboratory Medicine IT connectivity.
		2. The Laboratory Medicine IT Manager is responsible for ensuring that the laboratory LIMS is developed and maintained and for coordinating all upgrade activities to ensure that service disruptions and impact on service users is kept to the essential minimum and they are the conduit through which communication on all IT matters is escalated up to Trust IT or downwards from Trust IT to departments as appropriate. They will ensure that effective communication is established and sustained between the Trust IT leads and key laboratory staff and management whenever there are IT incidents that impact on Laboratory Medicine services. They will lead on the response to incidents and orchestrate appropriate resolutions. They will ensure that effective and timely communication is maintained during and following the resolution of incidents and that this reaches all appropriate staff members.
		3. Although not exhaustive, the IT systems used within the Directorate of Laboratory Medicine are generally used for combinations of data collection, processing, recording, and the storage and/or retrieval of examination results, patient and department business and performance data.
		4. IT procurement includes hardware and software upgrades and replacements of part or whole systems. The Laboratory Medicine IT Manager is responsible for coordinating these activities under the direction of the Laboratory Medicine Executive and/or individual Laboratory Managers/ Clinical leads as appropriate to the level of requirement. The laboratory Medicine IT Manger will ensure that there is a current documented procedure for the selection and purchasing of external IT services and this includes approval processes. The Laboratory Medicine IT Manager will orchestrate the processes and may delegate responsibilities to department IT leads as required. The Laboratory Medicine IT Manager will ensure that appropriate service level agreements are maintained and can be produced for inspection/audit and will liaise with Laboratory Managers and appropriate Trust IT management to maintain this requirement.
		5. The IT systems used must have manufacturer **validation information** that will be subsequently **verified** by Laboratory Medicine prior to use. The Laboratory Medicine IT Manager will lead on these processes and will liaise and collaborate with Trust IT and Laboratory Medicine individual department IT leads as necessary. Although accountable for this activity, the laboratory Medicine IT Manager may delegate appropriate responsibilities to other IT leads within the directorate. Although not exhaustive validation and verification will apply to the following areas:
1. Proper functioning of interfaces and middleware between the laboratory analytical systems and LIMS.
2. Proper functioning of interfaces and middleware between the laboratory LIMS and hospital and other service user’s patient administration systems (both primary and secondary care).
3. Proper functioning of personal computers, tablets, smart devices and electronic reporting systems.
4. Proper functioning of all systems described above following upgrades of hardware or software or following repairs to either. Full validation would include end to end traceable connectivity, with a random check(s) being conducted at service user(s) location(s).
5. Proper functioning following the introduction of new techniques, methods, parameters and processes.
	* 1. The IT systems must be protected from unauthorised access, are safeguarded against tampering or loss and are operated in compliance with supplier specifications and all legislation regarding data protection. The Laboratory Medicine IT Manager is responsible for ensuring that these measures are in place and will seek the support of Trust IT and IT Governance to ensure that all requirements are met and all data processed conforms fully to the requirements of the Data Protection Act i.e. It is:
6. Used fairly and lawfully.
7. Used for limited, specifically stated purposes.
8. Used in a way that is adequate, relevant and not excessive.
9. Accurate.
10. Kept for no longer than is absolutely necessary.
11. Handled according to people’s data protection rights.
12. Kept safe and secure.
13. Not transferred outside the UK without adequate protection
	* 1. The IT systems must operate in a manner that ensures the full confidentiality of data/information is maintained at all times. The Laboratory Medicine IT Manager is responsible for ensuring that these measures are in place and will seek the support of Trust IT and IT Governance to ensure that all requirements are met.
		2. The Laboratory Medicine IT Manager is responsible for ensuring that all appropriate documentation to permit systems operation is current, documented and available to all authorised users and is subjected to the document control requirements of the Directorate of Laboratory Medicine Quality Management Systems.
		3. The Laboratory Medicine IT Manager is responsible for ensuring that systems are in place to ensure the accurate representation and ongoing transfer for all examination results and associated clinical and technical comments, whether reproduced in hardcopy (printed) or electronic format. The Laboratory Medicine IT Manager may delegate responsibilities to department and other IT leads as necessary. Audits will ultimately be approved by the Laboratory Medicine IT Manager who will ensure that corrective and remedial actions are progressed for all nonconformities identified. The Laboratory Medicine IT Manager will instigate a pre-planned schedule of audits for IT and will present progress against these at Laboratory Medicine Board Meetings.
		4. The Laboratory Medicine IT Manager will devise and instigate a programme of scheduled audit to measure the functionality of system dynamics and compliance with expectations. The audits may be delegated to Laboratory Medicine department IT Lead’s to undertake. Non conformities generated from audit must be addressed and completed as soon as possible after discovery.

Where information systems are managed and/or maintained by third parties on behalf of the Directorate or subcontracted to alternative providers, the Laboratory Medicine Board shall ensure through service level agreement, that the provider meets all regulatory and legislative requirements. This may be delegated through the Laboratory Medicine IT Manager.

**Laboratory IT Failure(s)**

* + 1. Although not exhaustive, Laboratory IT systems will include the following types:
1. Personal Computers (PC’s)
2. Interfaces and Middleware systems
3. Laboratory LIMS (iLab)
4. Telephones (including authorised smart phones)
5. Tablets
6. Projection Equipment
7. All Computer Hardware belonging or leased to the laboratories that is not covered by the points above.
8. All software belonging or leased to the laboratories that is not covered by the points above
	* 1. If the IT failure can be resolved by the user then this should be done immediately e.g. local power failure where the system simply needs to be rebooted.
		2. If the IT issue cannot be resolved then the incident should be reported to the department IT lead who will investigate and apply appropriate corrective and remedial actions. They will advise laboratory staff and laboratory management appropriately depending upon the severity of the incident(s) and their impact on the laboratory services. The laboratory IT lead will escalate the issue
		3. The laboratory IT lead will escalate the issue through to the Laboratory Medicine IT Leads appropriately e.g. for situations that can impact on the Directorate ability to provide services. They will take direction from the Laboratory Medicine IT leads and liaise closely with them to put into effect appropriate resolutions within accepted time frames and to ensure that communication is cascaded to all appropriate staff groups at all levels.
		4. For major LIMS and other IT failures that impact only on the Directorate and not beyond, the Laboratory Medicine, the Directorate IT Manager or deputy must be informed and they will orchestrate the response to the failure, notifying the Trust IT if appropriate. They will ensure that timely and effective communication is maintained until recovery has been achieved.

**Trust Level IT Failure(s)**

* + 1. Trust Level failure (s) will be managed in accordance with ‘The Newcastle upon Tyne Hospitals NHS Foundation Trust Business Continuity Management Policy’.
		2. Minor IT issues that do not impact on the functionality of Laboratory Medicine departments or on the directorate, can be reported to the Trust IT help desk (contact details on the Trust intranet).
		3. For other less severe issues that impact on individual departments, the Laboratory Medicine IT Leads will be the initial contacts to facilitate recovery of services that impact on the department. The laboratory Medicine IT manager or deputy will work hand in hand with Trust IT leads to facilitate recovery of Laboratory Medicine IT systems in full accordance with the Trust Business continuity Policy and the Department Business Continuity Plan. In the absence of the Laboratory Medicine IT Manager or deputy, individual department IT should collaborate on the response process.
		4. The Laboratory Medicine IT lead will orchestrate the department recovery plan and will liaise directly with individual department IT leads and department Clinical and Management Leads to ensure a cohesive and coordinated response takes place within the time frames stipulated in the recovery plan.
		5. The Laboratory Medicine IT Leads will ensure that following corrective and remedial actions for IT failure, systems are reactivated in the correct sequence within the Directorate and will coordinate the tasks of the individual department IT leads in this process.
		6. The Laboratory Medicine IT Manager or deputy will ensure that timely and effective communication is maintained between the laboratories and the Trust IT department as necessary until full recovery is achieved.
		7. Laboratory Medicine Department IT leads will ensure that the recovery strategy is carried out under the direction of the Laboratory Medicine IT Manager or deputy and they will coordinate activities within their departments and ensure effective and timely communication is maintained at all times until recovery is fully achieved. They will coordinate the recovery processes and ensure that all systems are re-engaged in the correct systematic order.

**IT Business Continuity Plan**

* + 1. The Laboratory Medicine IT Manager is responsible for ensuring that there is an IT Business Continuity Plan for the management and recovery of IT disruption and for ensuring that it is subjected to document review as part of the Directorate Quality Management systems and periodic scheduled audit to test its continued appropriateness. Reference will be made to the Trust Business Continuity Policy to ensure that it continues to meet Trust requirements. Although not exhaustive the recovery plan will include the following points:
1. A list of services, equipment and systems that could be affected.
2. Maximum tolerable disruption times.
3. Recovery time objectives (should be less than point ii above).
4. Assessment of impacts of disruptions (e.g. reports, testing, communication etc.).
5. Identify critical processes and data (Middleware, Voice and written communication systems etc.).
6. Other critical support services (internal and external to the organisation).
7. Identify minimum resources required.
8. Assessment of likely workload ‘backlogs’ and workload priorities (e.g. urgent and routine).
9. Assessment of ‘time’ impact on response i.e. routine and non-routine hours of work.
10. Appropriate risk assessments be commissioned and in place (may be delegated to department IT leads).
	* 1. Although not exhaustive the IT Business Continuity plan will include the following points:
11. Purpose and scope of plan
12. Owner (directorate / departmental manager) and maintainer of plan (business continuity lead)
13. Details of staff roles and responsibilities in plan
14. The directorate / department process for invoking the plan and escalating to the Corporate Team in and out of hours.
15. Essential staff, support service and supplier contact details
16. Incident Management plan. In the context of the Trust plan, document the directorate / department action and tasks required to manage the initial phase of the incident. This should describe essential communications.
	* 1. The Laboratory Medicine IT Manager will ensure that Plans are stored in both electronic and paper formats in accordance with Trust requirements (Section 8 of the Trust Business Continuity Policy).
		2. The IT Business Continuity Plan is intended to ensure the safety of patients through maintaining the quality of service and that all statutory and regulatory obligations are met. It is intended to ensure that contractual requirements are maintained with minimum revenue loss and that all necessary actions are taken to ensure a successful recovery outcome within the shortest possible time frame.

**IT and Communications Applications and Data Recovery Requirements**

* + 1. The tables below show the recovery requirements for IT systems, data and communications for the individual departments in Laboratory Medicine:
		2. **Blood Sciences**
1. *Applications*



1. *Hardware Requirements*



1. *Communication Requirements*



* + 1. **Cellular Pathology**
1. *Applications*



1. *Hardware Requirements*

**

1. *Communication Requirements*



* + 1. **Microbiology**
1. *Applications*



1. *Hardware Requirements*

**

1. *Communication Requirements*



**Laboratory Medicine Intranet and Web Sites**

* + 1. The Directorate of Laboratory Medicine will ensure that the information provided to service users and other authorised personnel/organisations is current, accurate and complete. The Laboratory Medicine IT Manager is responsible for ensuring that the systems meet with these requirements and will undertake regular audit to ensure compliance and instigate appropriate corrective actions where they do not. They will be the point of contact for change requests but may delegate responsibility for progression to department IT leads or other authorised personnel within the directorate.
		2. Where changes to the web/intranet sites are necessary, the initial request should be made to the individual department IT lead. They will inform the Laboratory Medicine IT Manager and will escalate as appropriate and in a timely manner. Minor changes may be carried out immediately but major changes to the layout and presentation will require ratification by the Laboratory Medicine Board. The Laboratory Medicine IT Manager may administrate and facilitate the process but will not necessarily carry out the specific changes. The specific alterations will be undertaken by people with the appropriate authority to instigate this in the various departments within the directorate e.g. clinical and technical leads.
		3. All Managers, Clinical Leads and Section Leaders are required by the Trust to take ownership of and to seek to improve the quality of information within their services and they should be proactive in this endeavour.

**Confidentiality**

* + 1. The Laboratory Medicine IT Manager is responsible for ensuring that all Directorate IT systems operate in compliance with Trust Confidentiality and Security requirements and they will liaise with Trust IT and IT Governance leads as necessary to achieve requirements. They will instigate appropriate actions where directorate systems are noncompliant and will delegate responsibilities appropriately to Laboratory Medicine department IT leads and other authorised personnel as necessary.
		2. The Laboratory Medicine IT Systems shall operate in full compliance with Data Protection and Caldecott Guidelines and the current Trust policy should be read in conjunction with this document.
		3. All members of staff employed whether permanently or otherwise and third part staff operating on behalf of the Directorate of Laboratory Medicine must conform to the confidentiality requirements stated in this policy.
		4. All personally identifiable information is regarded by the Trust as confidential and all staff must make every effort to prevent this being seen by none authorised personnel. Staff members must be aware of non-authorised persons being in the near vicinity of such data and they must take necessary steps to ensure confidentiality is maintained.

**Audit**

* + 1. The Laboratory Medicine IT Manager is responsible for ensuring an ongoing programme of planned IT audit is implemented within the Directorate.
		2. Specific IT audit of individual sections is conducted against a planned schedule. This is undertaken by the IT Manager and/or designated deputies, the department IT leads in attendance with section and clinical leads for individual sections within Laboratory Medicine. This audit is intended to test the functionality and effectiveness of all Directorate IT systems and processes and to measure compliance against expectations. The record of audit will be held on Q-Pulse and is intended to provide data on holistic outcome. All nonconformities will be investigated and brought to the attention of department management for any corrective and necessary actions
		3. Ad hoc audit is at the discretion of the auditor but should follow the same general progression as detailed above. Typically audit should be used to monitor compliance and effectiveness following software and hardware upgrades and should be applied to measure true ‘end to end’ connectivity. The auditor must measure effectiveness by physically visiting end user(s) result IT stations.
		4. The auditor should target/examine specific components where nonconformity is suspected as opposed to areas where compliance is fully expected. This will give a true reflection of where nonconformities and therefore risk exists and is the main purpose of the audit process.
		5. All audit findings and corrective actions should be completed within an agreed and reasonable timeframe. The Laboratory Medicine IT Manager will monitor compliance and ensure closing of audit findings in a timely manner. These will formulate part of a quarterly report to the Laboratory Medicine Clinical Governance and Quality. All failings in this area will be reported to Clinical Director for Laboratory Medicine, Individual Department Clinical Leads and Laboratory Managers and to the Clinical Governance and Quality Lead for Laboratory Medicine. The Clinical Director of Laboratory Medicine has Executive authority to ensure that all appropriate actions are taken to remedy nonconformities.

A copy of the Audit report should be sent to department IT leads who will present the summary at department Clinical Governance and Quality Committee Meetings.

**Documentation and Document Control**

* + 1. There shall be current, valid and accurate documents available to authorised members of Laboratory Medicine personnel that describes the functionality and day to day use of the IT systems. These documents should be controlled in accordance with Laboratory Medicine Policies and this includes being subjected to periodic reviews and approval mechanisms. The Laboratory Medicine IT Manager is responsible for ensuring that these documents and their control processes are in place but is not necessarily the owner or ultimate approver. Document ownership will vary with level and the Laboratory Medicine IT Manager will appropriately delegate responsibility for documents that apply at department level.
		2. Although not exhaustive the types of documents and responsibilities for update and review would be expected to include:
1. SOP’s that describe the use and functionality of the LIMS – *Laboratory Medicine IT Manager*
2. Policies relating to the LIMS - *Laboratory Medicine IT Manager*
3. SOP’s that describe the LIMS functionality and application in specific departments, sections and procedures (e.g. authorisation of results in specific sections of specific departments) – *Department IT Leads*
4. Risk assessments (depending upon application level) - *Laboratory Medicine IT Manager and/or Department IT Leads*
5. Reports to the Laboratory Medicine Board - *Laboratory Medicine IT Manager*
6. Reports to Individual department boards - *Department IT Leads*
7. Verification and Validation documents- *Laboratory Medicine IT Manager*
8. Audit - *Laboratory Medicine IT Manager and/or Department IT Leads*

**Validation and Verification**

* + 1. All IT upgrades (either hardware and/or software) will be fully validated and verified. The Laboratory Medicine IT Manager will lead on this and will coordinate the response and delegate individual tasks within designated time frames to this end.
		2. All validation and verification documentation will be retained in accordance with directorate protocols and policies for document retention.

**Nonconformities and Complaints**

* + 1. The Clinical Director for Laboratory Medicine is ultimately responsible for ensuring that nonconformities and complaints are investigated and acted upon. The Clinical Director will delegate investigation responsibility appropriately and dependent upon the severity of the incident.
		2. The Laboratory Medicine IT Manager will act as initial lead for IT nonconformity and complaint issues but will delegate appropriately to department IT leads as required. The Laboratory Medicine IT manager will appraise the Clinical Director of Laboratory Medicine and the Clinical Governance Lead for Laboratory Medicine of all major IT incidents that impact upon services. They in turn will ensure that all appropriate key department personnel are informed.
		3. Incidents must be escalated in accordance to Trust and Laboratory Medicine policies and full root cause investigations undertaken as necessary with corrective and remedial actions implemented appropriately. The Laboratory Medicine Clinical Governance and Quality Committee will ensure that all nonconformities are investigated and the findings reviewed in a timely manner with corrective and remedial actions implemented and tested for effectiveness. The Laboratory Medicine Clinical Governance and Quality Committee will delegate one of its members to lead on any investigation as appropriate.
1. **Training**

This policy is part of the Directorate of Laboratory Medicine strategy and all staff are expected to familiarise themselves with its content. The policy is freely available through the document control system (Q-Pulse) and electronic acknowledgment (electronic signature) is taken as a record of a staff member having read and understood the policy contents.

All staff members must adhere to ethical principles when applying this policy and must adhere to NHS, Trust and professional codes of practice when carrying out their duties.

* 1. **Mandatory**
		1. It is a mandatory training requirement that all staff members in the department who operate IT systems have appropriate training and competency to do so. All staff must acknowledge that they have read and understood the contents of any SOP or policy associated with this (using the integral electronic signature facility on Q-Pulse), before they carry out any procedure that the SOP or policy relates to.
		2. Information Governance training is an annual mandatory requirement for all employees in the Trust. This can be undertaken through the Trust Intranet (online) and compliance is monitored by Human Resources. There are no exceptions to this requirement and all staff members have a duty to comply
	2. **Non-mandatory**
		1. There are no other specific requirements applying to this policy.
1. **Process (s) *for monitoring compliance with the* policy/procedure*. (This section is optional for strategy documents.)***

The method adopted for monitoring compliance will depend on the policy/procedure type but may include the following:

1. Sample audits of patients views/experiences
2. Staff surveys to assess knowledge, implementation and experience of policies
3. Health and Safety and ward/environmental inspections and audits
4. Monitoring adherence to policies via performance management programmes/appraisals

The Laboratory Medicine IT Manager produces quarterly incident, accident, non-conformities and non-compliance reports and also an annual report incorporated into the Laboratory Medicine annual management review.

1. Monitoring of ethnicity and diversity and equality legislation where appropriate
2. Meeting minutes / other evidence demonstrating effective functioning of arrangements as

Outlined within the policy.

Where a committee is nominated to review the policy / procedure compliance then that committee should also be consulted as part of the development and ratification process.

|  |  |
| --- | --- |
| ***Standard / process / issue***  | ***Monitoring and audit***  |
| ***Method***  | ***By***  | ***Committee***  | ***Frequency***  |
| * CPA standards for the Medical Laboratory
* ISO15189 Standard for the Medical Laboratory
* Blood Safety and Quality Regulations (BSQR) 2006
* Care Quality Commission Standards for provider quality checking
 | Scheduled program of audit for The Directorate of Laboratory Medicine Quality Management System.Scheduled program of audit for The Directorate of Laboratory Medicine Quality Management System.Scheduled program of audit for The Directorate of Laboratory Medicine Quality Management SystemScheduled program of audit for The Directorate of Laboratory Medicine Quality Management System | Quality Manager or devolved responsibility to Quality and Training team member.Quality Manager or devolved responsibility to Quality and Training team memberQuality Manager or devolved responsibility to Quality and Training team memberQuality Manager or devolved responsibility to Quality and Training team member | The Directorate of Laboratory Medicine Clinical Governance and Quality Committee.The Directorate of Laboratory Medicine Clinical Governance and Quality Committee.The Directorate of Laboratory Medicine Clinical Governance and Quality CommitteeThe Directorate of Laboratory Medicine Clinical Governance and Quality Committee | Monthly program of Quality Management Audit.Monthly program of Quality Management Audit.Monthly program of Quality Management Audit.Monthly program of Quality Management Audit. |

1. **Consultation and Review**

When reviewing a strategy/policy/ procedure all appropriate subject specific guidance will be taken into account. In addition to relevant subject specific guidance, the requirements of regulatory bodies e.g. the Care Quality Commission (CQC), the NHS Litigation Authority (NHSLA), Health & Safety Executive (HSE), United Kingdom Accreditation Service (UKAS), Medicines and Health Regulatory Agency (MHRA) and Department of Health will be taken into account and noted within this section. This list is not exhaustive and may alter in accordance to guidance and legislation changes.

The involvement of all groups, committees, forums and stakeholders responsible for ensuring the safe and effective implementation of strategies, policies and procedures are key to the review and development of effective documents. Stakeholders will be asked to contribute, comment and agree the content of a document before it is passed to the appropriate body for approval.

A decision will be made by the approving body on the appropriateness of involvement of each group depending on the nature of the strategy/policy/procedure being developed or reviewed. A list of the persons or groups from whom comments have been invited should be included in this section.

1. **Implementing (including raising awareness)**

This document will be distributed through Q-Pulse and all staff will be notified of its existence and their acknowledgement of receipt will be audited by the Quality Management teams in each laboratory discipline and non-compliances will be policed and acted upon by the Laboratory Medicine IT Manager and/or department Quality Manager(s) to ensure that all requirements are fulfilled.

1. **References**
2. ISO 15189 standard for the Medical Laboratory.
3. Care Quality Commission standards
4. BSQR 2006
5. Data Protection Act
6. **Associated documentation**

There are a number of Trust policies that apply to accident and incident reporting and investigation and the links are provided below:

* NUTH Business Continuity Management Policy

[**http://nuth-vintranet1/apps/policies/operational/BusinessContinuity201303.pdf**](http://nuth-vintranet1/apps/policies/operational/BusinessContinuity201303.pdf)

* NUTH Information Governance Policy

[**http://nuthvintranet1/apps/policies/InfoAndResourcePacks/InformationGovernancePolicy201103.pdf**](http://nuthvintranet1/apps/policies/InfoAndResourcePacks/InformationGovernancePolicy201103.pdf)

* NUTH Confidentiality and Security (Data Accreditation) Policy

[**http://nuthvintranet1/apps/policies/InfoAndResourcePacks/InformationGovernancePolicy201103.pdf**](http://nuthvintranet1/apps/policies/InfoAndResourcePacks/InformationGovernancePolicy201103.pdf)

* Reporting Incidents and Accidents

[**http://intranet.xnuth.nhs.uk//Policies/accidents/AccidentsIncidentsReporting201204.pdf**](http://intranet.xnuth.nhs.uk//Policies/accidents/AccidentsIncidentsReporting201204.pdf)

* Incidents and Accidents Disciplinary Policy

[**http://intranet.xnuth.nhs.uk//Policies/accidents/IncidentsAccidentsDiscipline201312.pdf**](http://intranet.xnuth.nhs.uk//Policies/accidents/IncidentsAccidentsDiscipline201312.pdf)