NHS
London North West
University Healthcare
NHS Trust

Digital Policy

Policy Number:	LNWUHT/CorpQRG/May08/2018
Name of ratifying committee:	Corporate Quality & Risk Group
Date Ratified:	1st March 2018
Date issued:	May 2018
Review Date:	April 2021
Responsible Executive Director	Simon Crawford, Director of Strategy and Deputy Chief Executive
Name of author:	Sonia Patel, Chief Information Officer
Name of approving committee and date of approval	Corporate Quality & Risk Group
Name of review Group/Committee:	Corporate Quality and Risk Committee
This policy has considered the Trust HEART Values:	☒ Honesty ☒ Equality ☒ Accountability ☒ Respect ☒ Teamwork
Equality Impact Assessment Outcome	None
Which stakeholders have been consulted? (refer to section 8 of the Policy on Policies)	Executive Directors, Committee members
Target audience:	Trust wide
Associated documents/policies:	Major Incident Policy

Relevant legislation:	• Data Protection Act 1998 • Freedom of Information Act 2000 • Computer Misuse Act 1990 • Confidentiality NHS Code of Practice 2003 • Caldicott Principles (latest revision 2013) • Copyright, Designs and Patents Act 1988 • General Data Protection Regulation 2017 • Information Governance Toolkit v14.1 2017-2018 • Copyright, Designs and Patents Act 1988 • Civil Contingencies Act 2004 • Human Rights Act 1998 • Regulation of Investigatory Powers Act 2000
Were comments sought from the Counter Fraud Service with regard to fraud and bribery?	N/A
Version Control	
Version number:	
Type of change/new policy:	New policy, replacing existing IM&T policies on IT Security, Data Protection and Freedom of Information.
Brief description of change:	Consolidation of IT policies into one. Additional statements around the selection and introduction of changes to systems.

TABLE OF CONTENTS

1 INTRODUCTION

1.1 INTRODUCTION

1.1.1 We live in a Digital world where Information Technology (IT) pervades all areas of the Trust and staff are reliant on it for accessing patient information, communicating and operating equipment. There are risks inherent with the use of digital technology around loss of information or failure of Trust processes. In order to reduce the impact and likelihood of these risks staff are required to follow the standards set out in this policy.

1.2 POLICY STATEMENT

1.2.1 This policy details the standards that must be maintained (both individually and corporately) to use the Trust's Digital services (the IT infrastructure and systems) in a safe and secure manner, minimising the risk of loss of information or disruption to Trust services.

1.2.2 Breach of any standards in this policy may result in an investigation that could result in disciplinary action being taken in accordance with the Trust's disciplinary policy. In the event of a breach occurring, the ICT access of the member of staff or contractor involved may be immediately suspended pending the conclusion of the investigation.

1.3 SUMMARY OF POLICY

1.3.1 The diagrams attached summarise the layout and standards in this policy. They should be used as an additional reference and reminder of the policy and should not be used in place of reading the policy.

1.3.2 Each section of this policy has an introduction describing what it covers and who the section applies to.

1.4 RATIONALE

1.4.1 The departments within the IT directorate (see definitions below) are focused on protecting staff and patient information and on making Trust activities as efficient and productive as possible. They do this through enforcing this policy and through the various products and services that they offer.

1.4.2 However, the IT directorate cannot do this alone and all Trust staff (including students, visitors and contractors) have a responsibility to read and follow this policy.

1.4.3 The Trust's IT Service Desk system ("Top Desk") and other documentation provide additional information that will help staff understand and sign up to the elements of this policy.

1.5 PURPOSE OF POLICY

1.5.1 The purpose of this policy is to set out the standards that must be followed across the use of, and management of, IT equipment and systems.

1.6 SCOPE OF POLICY

1.6.1 This policy covers the Digital environment: the technical infrastructure in use as well as the systems that people access to do their day-to-day roles. This policy also covers the legislation in place to protect the rights of staff and the public, such as the Data Protection Act.

1.6.2 This policy covers the following areas of functional scope:

- **Acceptable use** of IT: the standards that should be followed in general use of the Trust's systems and infrastructure.
- How **Access** to systems and services is requested granted, including requirements around user names and passwords.
- Standards around the selection and implementation of **new systems**.
- **Change management** standards so that changes to systems and the infrastructure are carried out in a well-planned and secure manner with minimal disruption to Trust services.
- Standards to be followed which relate directly to the security of infrastructure and systems, to protect from a **Cyber**-**attack**.
- Standards to be followed which ensure that the Trust complies with the **General Data Protection Regulation** (GDPR) and **Freedom of Information** Act (FOI).
- The standards will also specify where a member of staff's own equipment can be used: **BYOD** (Bring Your Own Device).
- Issues arise with IT and systems, many times out of the direct control of the Trust. Therefore, all staff should know how to respond in an **emergency/disaster** situation and how to **continue business** as usual.

1.6.3 In accordance with the Trust's Policy on Policies, it details the following areas:

- Roles and responsibilities
- Related legislation
- Implementation of the policy
- Monitoring and audit of compliance
- Equality impact assessment

1.6.4 The application types covered by this Policy include:

- **Clinical systems** - such as ePro, PAS, PACS, etc. Clinical systems store Patient Identifiable Data and this information may be sensitive.
- **Common** Office systems such as email and Word. Individual emails may contain person/patient identifiable information or confidential information.
- **Technical/specialist** systems - such as those used by specific departments including ICT, HR, finance and procurement. These systems store confidential information and may store information which is person identifiable or corporately sensitive.

1.6.5 This policy does not detail procedures, which will be written separately to ensure compliance with this policy.

1.7 RELATED LEGISLATION AND STANDARDS

1.7.1 This policy, and the audit/monitoring of its implementation, helps ensure compliance with a wide range of legislation and standards. These include:

- Data Protection Act 1998
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Confidentiality NHS Code of Practice 2003
- Caldicott Principles (latest revision 2013)
- Copyright, Designs and Patents Act 1988
- General Data Protection Regulation 2017
- Information Governance Toolkit v14.1 2017-2018
- Copyright, Designs and Patents Act 1988
- Civil Contingencies Act 2004
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000

1.7.2 Other Trust policies should also be referenced:

- Social Media Policy
- Standing Financial Instructions
- Records Management Policy

2 ROLES AND RESPONSIBILITIES

2.1 INTRODUCTION

2.1.1 This section describes the roles and responsibilities of every individual that interacts with the Trust's ICT infrastructure and systems.

2.2 CHIEF EXECUTIVE

2.2.1 The Chief Executive has overall responsibility for ensuring that the Trust has appropriate policies in place and that they are fully implemented and robustly monitored across the Trust.

2.3 DIRECTOR OF STRATEGY/DEPUTY CHIEF EXECUTIVE

2.3.1 Executive lead responsible for ensuring this policy is embedded across all operational areas of the Trust.

2.3.2 Act as the Senior Information Risk Officer (SIRO) for the Trust. The SIRO acts as an advocate for information risk on the Board/Executive Directors' Committee and in internal discussions, and will provide written advice to the Accounting Officer on the content of the annual Statement of Internal Control (SIC) concerning information risk.

2.3.3 Present this policy for ratification by the appropriate committee, both at its introduction and subsequently as it is reviewed/updated.

2.4 CHIEF INFORMATION OFFICER

2.4.1 Senior Lead for the policy, taking responsibility for the approval process and ensuring that appropriate consultation takes place with all relevant stakeholders beforehand.

2.4.2 Present this policy for approval by the appropriate committee, upon its introduction and periodically when it is reviewed.

2.4.3 Provide leadership to the IT directorate, developing and implementing the Digital Strategy and ensuring that operational services deliver to the agreed levels of service.

2.4.4 Ensure processes are in place to review supplier performance.

2.4.5 Provide professional leadership for all staff involved in the delivery of IT systems and services, including those whose line management is outside of IT.

2.5 EXECUTIVE DIRECTORS

2.5.1 Executive Directors, if they are members of the ratifying or approving committee, are responsible for reviewing this policy and providing feedback to the author and policy sponsor.

2.5.2 Executive Directors are responsible for ensuring that staff are made aware of this policy and how it relates to their role/department.

2.5.3 They are also responsible for ensuring that breaches of the policy are dealt with in accordance with this policy and the Trust's disciplinary policy.

2.6 HEADS AND MANAGERS OF CLINICAL, CORPORATE AND ADMIN DEPARTMENTS, CLINICAL DIRECTORS

2.6.1 Senior managers, if they are members of the approving committee or if their views are sought during the consultation stage, are responsible for reviewing this policy and providing feedback to the author.

2.6.2 Senior managers are responsible for ensuring that staff are made aware of this policy and how it relates to their role/department.

2.6.3 They are also responsible for ensuring that breaches of the policy are dealt with in accordance with this policy and the Trust's disciplinary policy, investigating such breaches as necessary.

2.6.4 Every system must have an Information Asset Owner (IAO). The owner (or sponsor) must lead on business decisions in relation to that system and should be a senior manager or department head in the Trust.

2.7 ALL MEMBERS OF STAFF AND USERS OF IT SYSTEMS (INCLUDING STUDENTS AND CONTRACTORS)

2.7.1 All staff/users are individually responsible for ensuring that they are familiar with, and comply with, this policy, including how it is relevant to their everyday role. Noncompliance with this policy could be used as evidence in a disciplinary investigation as per the Trust's disciplinary policy.

2.7.2 In the event of a staff member having a problem interpreting a policy, they must raise this with their line manager and the document author.

2.7.3 All Trust staff have the responsibility and right to raise concerns where policies and procedures are not being implemented as they should be, or where the implementation of such policies and procedures are having an unforeseen adverse effect on any person, clinical or operational practice or procedure.

2.8 IT DEPARTMENT HEADS (ICT, IG AND SYSTEMS)

2.8.1 IT department heads, or team leaders, are responsible for the administration, maintenance and management of the IT systems and ICT infrastructure in scope of this policy and under control of the IT department.

2.8.2 The Head of IG is also the Deputy SIRO for the Trust, working directly with the SIRO where appropriate.

2.8.3 They are responsible for ensuring that staff within their teams are adequately trained in the management and administration of the systems/infrastructure components and have access to supporting documentation and information from the supplier or other reputable source.

2.8.4 Ensure that KPIs relevant to the system are available and reported to the Chief Information Officer.

2.8.5 Work with other departments, e.g. finance, to support their system management resources and processes where that department has the administration (IAA) responsibility.

2.9 IT DEPARTMENT STAFF (ICT, IG AND SYSTEMS)

2.9.1 IT department staff acting as Information Asset Administrators (IAA), are responsible for the administration, maintenance and management of the IT systems and ICT infrastructure in scope of this policy and under control of the IT department.

2.9.2 As part of their IAA role, and for specific identified systems, IT staff may be responsible for ensuring that Trust staff are trained in the use of the systems and have access to supporting documentation and information through the Intranet or Service Desk system.

2.9.3 Provide access to appropriate available reports through the system and directly produce KPIs demonstrating the performance, reliability and availability of the system(s) for which they are responsible.

2.9.4 Work with other departments, e.g. finance, to support their system management resources and processes where that department has the administration (IAA) responsibility.

2.10 DEPARTMENTAL STAFF OUTSIDE OF IT WITH RESPONSIBILITY FOR THE MANAGEMENT OR OWNERSHIP OF IT SYSTEMS

2.10.1 Every system must have an Information Asset Owner (IAO) and Information Asset Administrator (IAA). The owner (or sponsor) must lead on business decisions in relation to that system and the IAA must lead on the management, development and support of the system.

2.10.2 Other Trust staff, where they act as IAAs, are responsible for the administration, maintenance and management of the IT systems in scope of this policy and under control of their department.

2.10.3 As part of their IAA role, and for specific identified systems, these staff may be responsible for ensuring that Trust staff are trained in the use of the systems and have access to supporting documentation and information through the Intranet or Service Desk system.

2.10.4 Provide access to appropriate reports through the system and directly produce KPIs demonstrating the performance, reliability and availability of the system(s) for which they are responsible.

2.10.5 Under guidance from the IT department, and with professional accountability to it, they should ensure that they have the technical skills to support their system management (IAA) responsibilities.

3 ACCEPTABLE USE

3.1 INTRODUCTION

3.1.1 The standards in the **Acceptable use** section of this policy define the appropriate use of systems and ICT services by staff to support the Trust's business activities including research, professional development and the delivery of patient care.

3.1.2 These standards apply to all users of Trust systems and ICT services.

3.2 PERSON IDENTIFIABLE DATA (PID)

3.2.1 Use of PID is acceptable for purposes that directly contribute to the safe care of the patient including diagnosis, referral and treatment. Information may be passed for example as content in clinical letters, or part of electronic storage mechanisms such as patient administration and clinical systems.

3.2.2 PID is also acceptable for purposes that directly relate to the management and employment of staff. For example, sickness records or employee records.

3.2.3 Where PID is to be used for secondary purposes e.g. service redesign or benchmarking, the data must be pseudonymised or fully anonymised in accordance with the Trust's Pseudonymisation Procedure, a copy of which is available via the intranet. The General Data Protection Regulations section of this policy contains more details on Pseudonymisation.

3.2.4 Any such requests for access must be authorised by the responsible Line Manager for the requesting work area, the Caldicott Guardian and the Deputy SIRO (Head of IG). Where pseudonymisation or full anonymisation cannot be achieved e.g. in older clinical systems, access must be restricted to identified authorised users operating within an isolated environment.

3.2.5 PID for secondary purposes should never be shared with any parties outside the organisation without an Information Sharing Agreement and/or at the explicit consent of the patient. All new or potential shares of information in this context must be agreed by the Information Governance Steering Group.

3.2.6 Sharing of PID that can lead to damage of the Trust's reputation or the breach of any individual's rights to privacy would be deemed to be unacceptable and may lead to disciplinary action.

3.2.7 If you are unsure if the information you are handling is PID, please contact your line manager or the IG Manager.

3.3 CORPORATELY SENSITIVE DATA

3.3.1 Corporate sensitive information would apply to non-person identifiable data that is confidential or not appropriate for the public domain (as determined by the Freedom of Information Act). Examples of this include detailed financial records, Serious Untoward Incidents (SUI) records, or audit, legal and contractual information etc.

3.3.2 Acceptable use of this type of information would include supporting activities such as:

- Complaints procedures
- New project plans
- Internal reports or audits
- Legal actions

3.3.3 All staff using the information must have the appropriate authority to do so as prescribed by their job description.

3.3.4 Sharing of corporate information that can lead to damage of the Trust's reputation or breach any individual's rights to privacy would be deemed to be unacceptable and may lead to disciplinary action.

3.3.5 If you are unsure whether the information you are handling is corporately sensitive, please contact your line manager or the IG Manager.

3.4 SOCIAL MEDIA

3.4.1 The Trust's Social Media Policy should be complied with at all times.

3.4.2 Social media services are web or app-based and provide a collection of various ways for users to interact, such as chat, messaging, email, video, voice chat, file sharing, blogging, discussion groups.

3.4.3 Social media sites are blocked by the Trust's firewall and access is not allowed for personal purposes. If you have a business need to access social media then you should discuss this with your line manager, the communications team and then ICT.

3.4.4 Users should be aware that, when interacting with others through social media (even for personal purposes), their views could be construed as the views of the organisation, or they could be interacting with patients of the organisation, and a professional business attitude should be used at all times.

3.5 INSTANT MESSAGING SERVICES

3.5.1 Instant messaging is a way of communicating from one user to another and differs from email in that the conversations happen in real-time and may not be saved for future reference.

3.5.2 Staff must not use PID in private Instant Messaging services or apps (e.g. WhatsApp or Facebook Messenger) for internal business purposes or for private use on Trust equipment.

3.5.3 Skype for Business is available as a Trust-approved Instant Messaging tool and may be used for this purpose.

3.5.4 The acceptable use standards for email, described below, apply equally to instant messaging.

3.6 EMAIL

3.6.1 The corporate email service used by the Trust for business purposes is NHSMail. This can be accessed from any Trust or non-Trust device, including tablets and Smartphones. Installing access to NHSMail on a non-Trust device will enforce encryption and passcode features on that device. If you do not wish to have these features enabled then do not set up the device for NHSMail access. Full details can be found on the NHSMail website.

3.6.2 Staff must not send, forward or open any material which may be considered to be libellous, pornographic, sexually explicit, or which includes hostile material relating to gender, sex, race, sexual orientation, religious or political convictions or disability, or incitement of hatred, violence or any illegal activity.

3.6.3 Staff who open an email containing any such material must inform the Head of Information Governance and ICT Service Desk immediately.

3.6.4 Email transfer of individual patient identifiable or business sensitive data/information should only be made where both sender and recipient are using the NHSMail system (email addresses ending in @nhs.net).

3.6.5 NHSMail is Government accredited to OFFICIAL status, approved for exchanging clinical information with other NHSMail and Government Secure intranet (GSi) users by the Department of Health and endorsed by the British Medical Association, Royal College of Nursing and Chartered Society of Physiotherapy. It is also authorised for sending to other email systems that comply with the SCCI 1596 standard.

3.6.6 Email addresses ending in the following are therefore secure for the exchange of patient data: @x.gsi.gov.uk; @gsi.gov.uk; @gse.gov.uk; @gsx.gov.uk; @pnn.police.uk; @cjsm.net; @scn.gov.uk; @gcsx.gov.uk, @mod.uk. This list is subject to change and the advice of the IG department should be sought if you wish to send restricted information to someone outside of the NHS.

3.6.7 Emails to patients containing their own medical details or other details relating to treatment or condition must only be sent under the following conditions and after approval by the Caldicott Guardian and/or Information Governance:

- The patient has given informed consent and this is recorded.
- The patient has been fully informed of the risks involved in receiving emails containing information about their own condition and treatment
- All relevant staff in the department are up to date with Information Governance Training
- The patient knows that they can stop email correspondence and how to do it
- The email explains how the patient can respond to the information, that the staff member's email is not monitored 24/7 and should not be used for any urgent communication.

3.6.8 Users should exercise caution when disclosing their email address to commercial organisations unless specific information/goods are requested, as this information may be passed to other organisations generating unwanted 'spam' mail.

3.6.9 Authorisation to access another user's email account must be granted by the owner of that email account. An individual can grant a right to view, delete and respond to emails on their behalf.

3.6.10 If a staff member requires urgent access to another's work (e.g. to cover for illness), authorisation must be provided by the line manager or other senior member of the Department, in order for the ICT Service Desk to arrange this.

3.6.11 Distribution of a programme, sound, picture or any other files that infringe copyright is not permitted.

3.6.12 The use of other internet-based email (e.g. Hotmail and Yahoo Mail) is not allowed. Access to all Internet email accounts will be prevented.

3.6.13 The Trust will record all email usage and, in support of an investigation, may make this information available to the investigating manager upon request from the HR directorate.

3.6.14 Email communications should conform to good business practice in terms of content and language used. Consideration should be given to the number of users that an email is sent to and the use of the To, CC and BCC fields. Emails to multiple members of the public should always make use of the BCC field to ensure that email addresses are not visible to other recipients of the email. The email trail should be checked, and if necessary edited, before forwarding or replying to an email. Appendix 2 has a full list of email best practice.

3.6.15 Attachments should only be opened if you know the sender or are expecting it.

3.6.16 Copies of sent and received emails should be stored appropriately in line with the Trust's **Records Management Policy**.

3.7 INTRANET

3.7.1 Use of the Trust's Intranet by staff should only be in support of the performance of their duties, authorised social use or to undertake research and investigations.

3.7.2 Unacceptable use includes:

- Posting of personal or third party private and confidential information on an Intranet page.
- For any purpose where the individual's use was for personal gain at the expense of the organisation's reputation or financial loss

3.8 INTERNET

3.8.1 Staff shall not access sites that use a peer-to-peer process for file sharing or participate in on-line gaming.

3.8.2 Downloading and installation of software from the Internet is not permitted, even if there are no user-licence implications, unless prior permission is given from the Associate Director of ICT/Head of ICT. Similarly, staff shall not upload or transfer files or software via the Internet, without express written permission.

3.8.3 Downloading of programmes, sound, picture or any other files that infringe copyright is not permitted, and storage and distribution thereof may also make the individual liable to prosecution.

3.8.4 Staff must not attempt to circumvent or compromise any security restrictions or privileges, such as password controls, anti-virus measures or blocked websites and email attachments.

3.8.5 If staff have concerns or questions on what is deemed inappropriate use, they should contact their line manager or Associate Director of ICT/Head of ICT.

3.8.6 The Trust will record all Internet usage and, in support of an investigation, may make this information available to the investigating manager upon request from the HR directorate.

3.8.7 The Trust applies additional content monitoring and filtering systems that will deny, and report, access to content that is unacceptable in the terms of this policy.

3.8.8 Staff must not access websites that contain any material which may be considered to be libellous, pornographic, sexually explicit, or which includes hostile material relating to gender, sex, race, sexual orientation, religious or political convictions or disability, or incitement of hatred, violence or any illegal activity.

3.8.9 The Trust notes that access to subject matter and sites of a potentially contentious nature may be appropriate in some areas of normal operation and/or in specific circumstances, e.g. sex education, youth advice, approved research, etc. but prior consent from your line manager must be obtained before accessing this material.

3.8.10 The IT department maintains a list of allowed and forbidden websites. Requests to add a website to either list must be made via the IT Service Desk.

3.8.11 If an employee accidentally accesses material of the type referred to above, or other material, which they feel may be considered of an offensive nature, they should note the time and web site address and exit from the site and then inform their line manager and the Service Desk immediately via email or Top Desk.

3.8.12 If an employee is in doubt about whether it is appropriate for them to access a site, they should obtain the written approval of their line manager before doing so.

3.9 STORAGE ON DEVICES

3.9.1 The Trust's network drives are for the storage of clinical and corporate data by authorised personnel only. No information should be stored on local drives (e.g. C drives).

3.9.2 No personal information, including photographs, videos etc. shall be stored on the Trust's network or local drives.

3.9.3 Removable media ("memory/USB sticks") shall only be used by staff who have an identified and agreed business need for them and have been supplied and authorised by the ICT Service Desk to ensure that devices have appropriate levels of encryption applied.

3.9.4 All incidents involving the use of removable media must be reported to the ICT Service Desk immediately.

3.9.5 Removable media, containing personal or patient identifiable or business sensitive data/information should be disposed of in line with the Trust's disposal policy.

4 ACCESS

4.1 INTRODUCTION

4.1.1 The standards in the **Access** section of this policy explain the rules around gaining access to systems and services, including requirements around user names and passwords.

4.1.2 The Trust has a duty to enforce a clearly defined Access Policy to ensure that all staff working on behalf of it have an appropriately controlled access authorisation process for the network and systems they require to complete their duties.

4.1.3 Where user accounts are authorised, all staff must adhere to the Acceptable Use Policy and Cyber Security sections of this policy. The User Registration Form must be signed as acceptance of this. An example can be found in Appendix 8 although the Service Desk system (Top Desk) should be used to request access.

4.1.4 These standards apply to all users of Trust systems and ICT services. Some sections apply to certain categories of users such as volunteers or those that work remotely.

4.2 USER NAMES AND PASSWORDS

4.2.1 It should be noted that not all systems will be able to **enforce** the password standards in this sub-section and therefore the user has responsibility to ensure that their password conforms to these standards even if the system will allow less secure passwords.

4.2.2 Similarly, some systems will not **allow** some of these standards to be followed (e.g. may limit password length to 5 characters). In this case, the user is allowed to disregard that particular part of these standards only.

4.2.3 User names will be defined by the System Manager (IAA) of the system being accessed and will be unique. It will usually be derived from the user's full name, although some systems may not support this approach and an alternative method may be used (e.g. employee number).

4.2.4 Generic user names are forbidden for systems containing personal, confidential or sensitive information. Generic network logons are allowed where this only gives access to the Trust's Intranet. Onward access to other systems (e.g. the Clinical Portal, NHSMail) requires a system-specific user name and password unique to the user.

4.2.5 User names, which are not generic, must not be shared or used by anyone other than the member of staff for which it was created.

4.2.6 Passwords will initially be assigned by the System Manager (IAA) of the system being accessed. It must be changed on first access by the user. Passwords must never be shared with anyone else. If a password becomes known by someone else, it must be changed immediately.

4.2.7 Different systems will enforce different rules for passwords. The following are the standards[1] that users should follow when setting their own password:

- Passwords shall be at least 8 characters long
- Passwords must contain at least four alphabetic characters (a…z)
- Passwords must contain at least two numeric characters (0…9)
- Passwords must contain at least two lower case and two upper case alphabetic characters
- Passwords must contain at least two special or non-alphanumeric characters
- Passwords must not repeat the same character more than twice in a row
- The password must be changed at least every 60 days.
- Passwords must not be repeated within 6 months of their first use.
- The password shall not be easily guessable by someone with a basic knowledge of the user or formed from common dictionary words. The following are examples of easily guessable passwords:
  - Containing “password”
  - The same as the user name
  - The same as the name of the user
  - The date of birth of the user

4.2.8 After three successive failed attempts to log in, the account shall be disabled and an alert raised to the Information Asset Administrator (IAA). The IAA shall reset the password after confirming the identity of the user. For some systems, this duty of the Information Administrator may be delegated to the ICT Service Desk.

4.2.9 If Single Sign-on, pass-through or a biometric is used, the password may be managed by the Single Sign-on application.

4.2.10 If the user suspects that their password has been compromised or requires their password to be reset, they should contact the ICT Service Desk for advice and guidance.

[1] NHS Digital Password guide 23rd May 2017

4.3 COMMON SYSTEMS ACCESSIBLE TO ALL STAFF

4.3.1 By virtue of becoming an employee of the Trust, a network logon is provided with a user name and initial password. The initial password must be changed on first use according to the password standards described above. The login is provided upon request from the line manager using the ICT Service Desk system and upon agreement of the individual to comply with this policy. An example of the user registration form can be found in Appendix 8 although the online Service Desk system (Top Desk) should be used to request access.

4.3.2 Access is thereby given to the Trust's IT network giving access to the following common systems without further logon:

- Microsoft Office including Word, Excel and PowerPoint
- Internet and Intranet access with onward access to websites that do not require a separate user name or password
- A personal network drive (H drive) for storage and retrieval of files and documents, a shared departmental drive and public drives.
- Printers

4.3.3 Some systems that are common or available for all users do require a further logon. This includes:

- NHSMail. This is a national application with the password rules set nationally. Local administration (not the full IAA role) is carried out locally by the ICT Service Desk.

4.3.4 Staff that access systems are deemed to have agreed to the standards set out in this policy.

4.4 SYSTEMS WITH RESTRICTED ACCESS

4.4.1 Access to all systems other than the common ones described above, is given on a need-to-use basis upon request by the user's line manager on their behalf to the appropriate Information Asset Owner (IAO). The login is provided upon agreement of the individual to comply with this policy and upon appropriate training for the systems being accessed.

4.4.2 A logon is provided with a user name and initial password. The initial password must be changed on first use according to the password standards described above.

4.4.3 Once access to the system is no longer needed (for example, if the user changes role or leaves the Trust) then the IAA should be notified so that the account can be disabled.

4.4.4 In these circumstances, the user must no longer access the system, even if the account has not yet been disabled.

4.4.5 Staff that access systems are deemed to have agreed to the standards set out in this policy.

4.5 NATIONAL SYSTEMS

4.5.1 Access to national applications shall be governed by the national policy pertaining to that application. National applications include, but are not limited to:

- NHSMail
- PDS (Spine)
- eReferral System (formerly Choose and Book)

4.5.2 All users issued with a smart card are responsible for complying with the terms and conditions as set out in the RA01 Form. Compliance will be monitored via line management arrangements, and Registration Authority Team audit. Any breach of these will be viewed as a disciplinary matter.

4.6 VOLUNTARY AND HONORARY ACCESS

4.6.1 All voluntary and honorary users of the organisation's network and applications must read and agree to this policy setting out the standards for Acceptable Use.

4.6.2 Voluntary and honorary staff require authorisation from the IAO to access restricted applications required to fulfil any aspects of their roles. Authorisation to access common applications will be available in line with standards described earlier.

4.6.3 Locum staff, who may arrive at short notice in the Trust and require access, will be required to certify their relevant training is up to date. The access process will be operated by IT and local managers and requires agreement to comply with this policy.

4.7 THIRD PARTY (SUPPLIER) ACCESS

4.7.1 Partner agencies or third party suppliers must not be given details of how to access the organisation's network and applications without permission from the ICT Security Manager.

4.7.2 Any changes to supplier's access requirements must be immediately sent to the IAA or ICT Service Desk so that the appropriate level of authorisation can be updated (or ceased) following approval of the change request from the IAO.

4.7.3 All suppliers and their associated employees and agents must read and agree to this policy setting out the standards for Acceptable Use.

4.7.4 Third party access will be time-limited dependent on the tasks that they are required to perform as part of their contract with the organisation. Access will be enabled by the ICT Service Desk or IAA at that start of the task. On completion of the task, access shall be disabled by the ICT Service Desk or IAA.

4.8 PATIENT AND PUBLIC ACCESS

4.8.1 Patient access: patients may be granted limited **supervised** access to their medical records held on the Trust's clinical systems to view information relevant to their care, as directed by their clinician.

4.8.2 Patient access will only be authorised by the Clinical Director following a request by the patient's lead clinician. Such access must be supervised by the lead clinician.

4.8.3 The Trust may in the future provide the facility for limited access to a patient-facing internet-based application such as Patient Knows Best. The level of access will be strictly controlled to ensure that privacy and confidentiality of all information on the system is maintained, in line with this Policy, the NHS Confidentiality Code of Practice and the Data Protection Act.

4.8.4 Public access: limited public access to the internet and public-facing extranet sites is being rolled out across the Trust. There are no service level guarantees for the availability of this service. All usage is at the risk of the member of the public.

4.8.5 Where 'Guest Wi-Fi' is enabled, an account will be available for the public to access the internet and extranet. This may be provided by a commercial organisation, who may charge for this service. Access details will be published locally.

4.9 REMOTE ACCESS

4.9.1 Remote access, whether fixed or 'roving' includes:

- Mobile users (e.g. Staff working across sites, visiting patient homes or who are temporarily based at other locations)
- Home workers (e.g. IT support, Corporate Managers, IT development staff, Clinicians)
- Non-NHS staff (e.g. Social Services, contractors and other third party organisations)

4.9.2 Remote access accounts enable users to have secure and resilient remote access to some of the organisation's information systems, maintaining appropriate standards of availability and confidentiality for all sensitive or patient identifiable information

4.9.3 In providing remote access to staff, the following high-level principles will be applied:

- The Server Manager will be appointed to have overall responsibility for each remote access connection to ensure that the organisation's Policies are applied
- The IAO will decide whether remote access should be available for their application(s).
- Remote access accounts will be restricted to the minimum services and functions necessary for individuals to carry out their roles

4.9.4 Remote access is subject to the same Access and Acceptable Use standards as for on-site access.

4.9.5 When accessing information remotely, staff must ensure that no other person obtains inappropriate access to that information. For example, accessing patient information in a café or on public transport may expose patient information to others and should be avoided.

5 NEW SYSTEMS AND INFRASTRUCTURE

5.1 INTRODUCTION

5.1.1 The standards in this section of this policy relate to the justification, specification, selection and implementation of **new systems and infrastructure**.

5.1.2 It is essential that these standards be followed before committing the Trust to additional expenditure. The Trust has a Business Case Review Group that will form part of the approval process for new systems.

5.1.3 No new system may be submitted to a Trust group or committee for approval, let alone procured, without prior discussion with and approval from the Chief Information Officer who will assess the idea against the Digital Strategy.

5.1.4 Any proposal for a new system must be sponsored by a senior manager carrying out the Information Asset Owner (IAO) role. With the exception of ICT infrastructure elements, this person should sit outside of IT. The sponsor must take the lead in all of the activities described here, with the assistance of IT.

5.1.5 The objective of following this set of standards is to ensure that the right decisions are made with regard the selection and implementation of new systems.

5.1.6 The stages to be followed are set out in this section. They are:

- Justification
- Specification
- Procurement
- Deployment
- Disposal of legacy system

5.1.7 The form in Appendix 3 should be completed to support compliance with this policy and to track progress through these stages.

5.2 JUSTIFICATION

5.2.1 The first stage in selecting a new system is to justify its purchase. This involves writing a business case detailing all of the costs and benefits. This must be presented to the IM&T Programme Review Group and IM&T Strategy Group for discussion and approval **prior** to submission to the Trust's Business Case Review Group or other group or committee.

5.2.2 It is important that a specific supplier should not be assumed at this stage, as there may be a choice of suppliers/systems. The purpose of the standards detailed here are to provide a robust, fair process to demonstrate impartiality in the selection process and to ensure that the most economically advantageous solution is chosen.

5.2.3 Business Cases must follow the template provided by the Trust's Business Case Review Group and should include the following areas:

- Strategic case: setting out the strategic drivers and context and reducing the longlist of options to a shortlist.
- Commercial case: detailing the procurement route available and the state of the market.
- Economic case: demonstrating that the proposal is good value for money for the Trust. This involves detailing the risks, benefits and costs. Cost must consider:
  - Capital and Revenue costs.
  - Costs across the lifetime of the system (usually 5 to 10 years for IT systems)
  - Supplier costs
  - Implementation costs (resources)
  - Ongoing costs
  - Any additional (pre-requisite) costs
- Financial case: demonstrating the affordability of the system. This must consider Capital charges and VAT as well as funding sources (internal and/or external).
- Management case: this details how the system would be implemented, including timescales and governance.

5.2.4 If Capital funding is required then this will also need to be approved by the Trust's **Capital Project Group.**

5.2.5 Pre-procurement engagement with any number of suppliers can take place to help inform the business case.

5.2.6 More complex and expensive business cases require more detail and may go through several stages from Strategic to Outline and then to Full Business Case. The Full Business Case is completed after the Procurement stage. Small, less expensive systems may not require a multi-stage approach or as much detail but should still cover all of the areas above.

5.2.7 The justification of a new system must consider current systems that provide the same, or similar, functionality and how those systems would be affected. If they are to be replaced then the costs, effort and timescales to do so must be included in the business case.

5.2.8 The justification must also consider the impact on current processes, systems and infrastructure. This should be discussed with IT. There may be additional costs involved to reduce this impact. Examples include: upgrading PCs/network, testing integration between systems, etc.

5.2.9 Once approved by the IM&T groups the business case can be submitted to the Trust's Business Case Review Group and other committees as appropriate. Depending on the value, Trust Board approval may be needed.

5.2.10 Once the business case has been approved, the next stage can proceed. The next stage can be initiated before approval of the business case but cannot finish before business case approval.

5.3 SPECIFICATION

5.3.1 The next stage is to specify the detailed requirements for the new system. This must be done so that it is possible to assess which option/system/supplier is the best and so that a detailed implementation plan can be drawn up. It may also influence the Full Business Case, providing clarification to some of the initial assumptions in earlier drafts.

5.3.2 It is the responsibility of the IAO or system sponsor to write the requirements specification. The IT department (and other stakeholders) will help with this, particularly in the technical requirements.

5.3.3 The document specification must contain the following requirements:

- Functional:
  - This will depend on the system and is focused on specifying the desired functionality.
- Configuration:
  - This set of requirements are concerned with ensuring that the system has the appropriate levels of configuration. This may include screen design, form development, user account setup, reports, etc.
- Technical:
  - The technical requirements will be around the infrastructure. Examples include PC spec, impact on network, how/where hosted, etc.
- Interoperability:
  - Any requirement to interface with other systems should be specified here.
- Support:
  - The service levels and support required should also be specified. For example is the system going to be used (and supported) 24/7?
- Information Governance:
  - Requirements around the security of the information held on the system also need to be specified.
- Implementation:
  - The final part of the specification should look at requirements for implementation: the amount of training required, data migration from an existing system, etc.

5.3.4 The specification needs to be signed off by the IAO, IT department and other identified stakeholders. Each aspect of the specification will need weighting so that its relative importance can be identified.

5.3.5 Supplier responses to requirements will need to be scored. Therefore document the minimum and desired requirements – this will allow responses exceeding the minimum requirement to be scored higher, allowing a greater differential between suppliers.

5.4 PROCUREMENT

5.4.1 Once approval has been given to proceed and once the requirements have been fully specified, the next stage is procurement. This involves selecting the preferred solution/system/supplier to meet those requirements.

5.4.2 The procurement must be in line with the Trust's **Standing Financial Instructions** (SFIs) which dictate the level of competition required and the process to be followed. Depending on the total cost of the system, this could vary from a full OJEU procurement to a 3-quotes process. Single Tender Waiver's may also be possible under certain circumstances (e.g. for an incumbent supplier).

5.4.3 The principles for procurement are:

- The procurement timetable and process is communicated in advance and kept to where possible.
- Open to all appropriate suppliers (may be limited to those on a specific framework).
- All bidders have access to the same information.
- All bids evaluated consistently and according to the documented evaluation process, which is based on the published requirements.
- Most Economically Advantageous Tender (MEAT) is selected (not necessarily the cheapest as cost is only one criterion)
- The procurement may be halted if required (e.g. if the cost envelope is going to greatly exceed that assumed in the Outline Business Case).

5.4.4 The Trust's procurement department must be consulted with to ensure that the procurement proceeds correctly with minimal risk of being challenged by any [losing] supplier. They will be aware of any suitable Frameworks that can be used in the procurement and other relevant legislation around communicating the result.

5.4.5 Some components of the procurement may be possible without further competition. This would apply where they are standard equipment already purchased by the Trust. Examples include end user devices and servers.

5.4.6 The procurement process must be documented and planned in advance of any formal tenders going to suppliers and then shared with them. Once formal procurement is underway, all communication with suppliers must be on an equal basis.

5.4.7 Once a preferred supplier has been selected, the Full Business Case must be completed and submitted through the appropriate governance structure for approval.

5.5 DEPLOYMENT

5.5.1 The management case of the Full Business Case (FBC) should contains details on how the new system will be implemented. Following approval of the FBC, the following actions must be taken to expand on this:

- A Project Initiation Document (PID) must be written to define the project in detail. See below for a guide on what it should contain.
- A Project Board (PB) must be set up to oversee the implementation. PRINCE2 practice should be followed. The PB should consist of representatives from users of the system, the supplier and executive/senior management sponsorship as well as the Project Manager.
- The Project Team should be formed with representation from the workstreams required to implement the system. The workstreams will be defined in the PID (see below).
- A Privacy Impact Assessment (PIA) must be written detailing the impact of the system on the privacy of individuals (staff or patients). This is a requirement of the General Data Protection Regulation. Appendix 12 contains a summary of what should be in the PIA.
- For each system (Information Asset), a System Level Security Policy (SLSP) must be written. The SLSP must contain a considered and specific view of the range of security policy and management issues relevant to the system and that may encompass a range of technical, operational and procedural security topics. Appendix 10 contains details on the contents of an SLSP.
- A Clinical Safety Officer must be assigned and a Clinical Safety Report must be written detailing the level of testing that has gone and providing assurance as to little or no negative impact on clinical safety through the introduction of the system. Appendix 11 contains details on the contents of the Clinical Safety Report.
- The flows of data within and between systems must be documented.

5.5.2 The PID should detail the following:

- The aims and objectives of the project
- How the project will be governed and what assurance will be put in place
- Project scope and exclusions
- Summary of the business case and project budget
- The project plan
- Risks, Assumptions, Issues and Dependencies (RAID) and how they will be managed
- The project controls: stages, cost and quality

- Tolerances within which the Project Manager can operate without recourse to the Project Board
- The workstreams required to implement the system. These should include some or all of the following:
  - Management and admin
  - Change, transformation and benefits realisation
  - Training
  - Testing (which should take place in a non-live environment)
  - Design, development and configuration
  - Information Governance
  - Reporting
  - Interfaces
  - Handover to Business as Usual (BAU): support and service management

5.5.3 Before new systems are introduced, a Privacy Impact Assessment (PIA) must be completed which takes into account whether this new process or system will:

- Allow personal information to be checked for relevancy, accuracy and validity
- Incorporate a procedure to ensure that personal information is disposed of through archiving or destruction when it is no longer required
- Have an adequate level of security to ensure that personal information is protected from unlawful or unauthorised access and from accidental loss, destruction or damage
- Enable the timely location and retrieval of personal information to meet subject access requests.

5.5.4 Further details on how to carry out a Privacy Impact Assessment can be provided by the Trust's Deputy SIRO and/or Information Governance Manager.

5.5.5 The deployment should proceed according to the plan with Highlight Reports produced either at Stage boundaries or on a regular basis. An Exception Report should be produced if a project tolerance is exceeded.

5.5.6 The supplier of the application shall supply a list of known errors ("bugs") with the application before it is deployed.

5.5.7 The supplier shall supply an upgrade plan which shall include the procedure for rolling back to the previous version.

5.6 LEGACY DISPOSAL

5.6.1 If a new system is replacing an existing system then plans must be drawn up to exit from the existing (legacy) system. The must consider the following aspects:

- Migration of data to the new system or to an archive
- Decommissioning of hardware (servers, PCs, etc)

- Ceasing contracts with the existing system (including consideration as to notice periods and termination clauses in contracts)

5.6.2 The policy for disposal of legacy systems is described more fully in the next section, Changes to Systems and Infrastructure.

6 CHANGES TO SYSTEMS AND INFRASTRUCTURE

6.1 INTRODUCTION

6.1.1 **Change management** standards are required so that changes to systems and the infrastructure are carried out in a well-planned and secure manner with minimal disruption to Trust services.

6.1.2 The objective of following this set of standards is to ensure that the right decisions are made with regard the changing of systems or infrastructure, addressing the impact on Trust services.

6.1.3 Change management covers a wide range of circumstances, including:

- New functionality in existing systems (requiring an upgrade of the system)
- Maintenance upgrades to existing systems
- Change in usage of a system (e.g. introduction to a new set of users)
- Moves of offices (involving move of equipment, ensuring network connectivity, telephony, etc)
- Major changes to configuration of a system
- Changes to service levels or contracts
- Changes to meet new legislation (e.g. GDPR)

6.1.4 In many ways, a change to a system is the same as introducing a new system. The main difference are:

- There is not usually a need to run a multi-bidder procurement process (unless the contract is at the end of its term).
- The scope is smaller than for a new system.
- The impact of the implementation of the change on Business as Usual activities and Trust services will generally be greater as the system is already in use and significant downtime may be required.

6.1.5 Requests for changes to the ICT infrastructure should be submitted to the Technical Advisory Group (TAG) for discussion and agreement. This group consists of senior technical IT staff.

6.1.6 If the cost involved is significant enough that a change in supplier may be preferential, this would be identified and considered in the options appraisal part of the Business Case. Procuring a new system may then be preferred and the New System section of this policy would apply.

6.1.7 It is essential that these standards be followed before committing the Trust to additional expenditure. The Trust has a Business Case Review Group that may form part of the approval process for changes that require significant expenditure.

6.1.8 No system change should be agreed without prior discussion with and approval from the Chief Information Officer who will advise on the best approach and options.

6.1.9 Any proposal for system changes must be sponsored by the Information Asset Owner (IAO) role. The sponsor must take the lead in all of the activities described here, with the assistance of IT.

6.1.10 The stages to be followed are set out in this section. They are:

- Justification
- Specification
- Procurement
- Deployment
- Disposal of legacy system

6.1.11 The form in Appendix 4 should be completed to support compliance with this policy and to track progress through these stages.

6.2 JUSTIFICATION

6.2.1 The first stage in planning a change to a system is to justify the change. If the change involves expenditure (either with the supplier or internally) then you must write a business case detailing all of the costs and benefits. This must be presented to the IM&T Programme Review Group and IM&T Strategy Group for discussion and approval **prior** to submission to the Trust's Business Case Review Group or other group or committee.

6.2.2 Any options must be considered and evaluated in the Business Case. This could include making the change at the weekend to minimise disruption or procuring expert resource to assist with the change.

6.2.3 Business Cases must follow the template provided by the Trust's Business Case Review Group and should include the following areas. For a relatively simple and inexpensive change the Business Case document may be quite short

- Strategic case: setting out the strategic drivers and context and reducing the longlist of options to a shortlist.
- Commercial case: detailing the procurement route available. For a change to an existing system, this will be trivial as the incumbent supplier will be the only viable option.

- Economic case: demonstrating that the proposal is good value for money for the Trust. Sometimes there is a contractual or legal requirement for the change. If so, this should be specified because the other benefits may not in themselves justify the change. This involves detailing the risks, benefits and costs. Cost must consider:
  - Capital and Revenue costs.
  - Costs across the remaining (or extended) lifetime of the system
  - Supplier costs
  - Implementation costs (resources)
  - Any change to ongoing costs
  - Any additional (pre-requisite) costs
- Financial case: demonstrating the affordability of the system. This must consider Capital charges and VAT as well as funding sources (internal and/or external).
- Management case: this details how the change would be implemented, including timescales, governance and impact on Trust services.

6.2.4 If Capital funding is required then this will also need to be approved by the Trust's **Capital Project Group.**

6.2.5 A system change may involve replacing current systems that provide the same, or similar, functionality. If they are to be replaced then the costs, effort and timescales to do so must be included in the business case.

6.2.6 The justification must also consider the impact on current processes, systems and infrastructure. This should be discussed with IT. There may be additional costs involved to reduce this impact. Examples include: upgrading PCs/network, testing integration between systems, etc.

6.2.7 Once approved by the IM&T groups the business case can be submitted to the Trust's Business Case Review Group and other committees as appropriate.

6.2.8 Once the business case has been approved, the next stage can proceed. The next stage can be initiated before approval of the business case but cannot finish before business case approval.

6.3 SPECIFICATION

6.3.1 The next stage is to specify the details of the change. This will allow a detailed implementation plan to be drawn up.

6.3.2 It is the responsibility of the IAO or system sponsor to document this, supported by information from a supplier (e.g. Release Notes). The IT department (and other stakeholders) will help with this, particularly with any technical changes.

6.3.3 The specification may contain detail in some or all of the following areas:

- Functional:
  - This will apply for system upgrades and will detail what functional changes are proposed. This may lead to requirements for training, etc.
- Configuration:
  - Changes to configuration need to be specified and planned. This may include screen design, form development, user account setup, reports, etc.
- Technical:
  - The technical requirements will be around the infrastructure. Examples include PC upgrades, use of mobile devices, network changes required, how/where hosted, etc. Infrastructure changes will be mostly technical and required much detail in this category.
- Interoperability:
  - Any requirement to change or implement interfaces with other systems should be specified here.
- Support:
  - Any changes to service levels or support required should also be specified.
- Impact on BAU:
  - The impact on Trust services needs to be detailed and planned for. This may involve system downtime, invocation of Business Continuity plans, etc.
- Implementation:
  - The final part of the specification should look at requirements for implementation: the amount of training required, data migration from an existing system, etc.

6.3.4 The specification needs to be signed off by the IAO, IT department and other identified stakeholders.

6.4 PROCUREMENT

6.4.1 Once approval has been given to proceed and once the changes have been fully specified, the next stage is procurement. This involves selecting the preferred solution/system/supplier to meet those requirements. For system changes, the incumbent supplier is likely to be the same and no procurement will be needed. For other changes, it may be required to procure new hardware or software.

6.4.2 Any procurement must be in line with the Trust's **Standing Financial Instructions** (SFIs) which dictate the level of competition required and the process to be followed. Single Tender Waiver's may need to be signed under certain circumstances (e.g. for an incumbent supplier).

6.4.3 The principles for procurement (if needed) are:

- The procurement timetable and process is communicated in advance and kept to where possible.
- May be open to suppliers or may only be appropriate for incumbent

- All bidders have access to the same information.
- All bids evaluated consistently and according to the documented evaluation process, which is based on the published requirements.
- Most Economically Advantageous Tender (MEAT) is selected (not necessarily the cheapest as cost is only one criterion)

6.4.4 If required, the Business Case must be updated and submitted through the appropriate governance structure for approval.

6.5 DEPLOYMENT

6.5.1 The deployment of a change is very similar to the deployment of a new system, although it may be a smaller project requiring few stages and resources.

6.5.2 The management case of the Business Case should contains details on how the new system will be implemented. Following approval of the Business Case, the following actions must be taken to expand on this:

- A Project Initiation Document (PID) must be written to define the project in detail. See below for a guide on what it should contain.
- A Project Board (PB) must be set up to oversee the implementation. PRINCE2 practice should be followed. The PB should consist of representatives from users of the system, the supplier and executive/senior management sponsorship as well as the Project Manager.
- The Project Team should be formed with representation from the workstreams required to implement the system. The workstreams will be defined in the PID (see below).
- Any changes to the system's Privacy Impact Assessment (PIA), System Level Security Policy (SLSP), Clinical Safety Report and Data Flow mapping.

6.5.3 The PID should detail the following:

- The aims and objectives of the project
- How the project will be governed and what assurance will be put in place
- Project scope and exclusions
- Summary of the business case and project budget
- The project plan
- Risks, Assumptions, Issues and Dependencies (RAID) and how they will be managed
- The project controls: stages, cost and quality
- Tolerances within which the Project Manager can operate without recourse to the Project Board
- The workstreams required to implement the system. These should include some or all of the following:
  - Management and admin
  - Change, transformation and benefits realisation
  - Training

- Testing (which should take place in a non-live environment)
- Design, development and configuration
- Information Governance
- Reporting
- Interfaces
- Handover to Business as Usual (BAU): support and service management

6.5.4 The deployment should proceed according to the plan with Highlight Reports produced either at Stage boundaries or on a regular basis. An Exception Report should be produced if a project tolerance is exceeded.

6.5.5 The supplier of the application shall supply a list of known errors ("bugs") with the application before it is deployed.

6.5.6 The supplier shall supply an upgrade plan which shall include the procedure for rolling back to the previous version.

6.6 EMERGENCY CHANGE REQUESTS

6.6.1 Changes to systems or to components of the IT infrastructure are sometimes required at short notice and without the time to go through the full process described above. Examples of this type of change are:

- A severe degradation of service needing immediate action
- A system/application/component failure causing a negative impact on business operations
- A response to a natural disaster
- A response to an emergency business need

6.6.2 Where emergency changes to systems and data are required, the event must be recorded and appropriate documentation and approvals obtained from the IAA, IAO and IT department as soon as possible after the event.

6.6.3 After the event, the policy should be complied with in retrospect.

6.6.4 If a further change is required after the initial emergency has been resolved, this change shall comply with appropriate non-emergency section of this Policy.

6.7 LEGACY DISPOSAL

6.7.1 If a new system is replacing an existing system then plans must be drawn up to exit from the existing (legacy) system. This is considered as a change in the current system. The must consider the following aspects:

- Migration of data to the new system or to an archive
- Decommissioning of hardware (servers, PCs, etc)
- Ceasing contracts with the existing system (including consideration as to notice periods and termination clauses in contracts)

6.7.2 The organisation has a responsibility to dispose of all ICT equipment safely and securely including the destruction of any information stored thereon.

6.7.3 In considering disposal of an ICT asset, the following must be considered:

- The reason why the asset should be disposed of (e.g. it has become unserviceable due to age, or it is beyond economic repair)
- The estimated market value of the item, taking account of professional advice where appropriate, for audit depreciation values

6.7.4 The senior IT manager for the area concerned (servers, networks or end user devices) will then ensure:

- A professional disposal company is engaged to destroy/recycle all condemned ICT equipment in line with regulatory and legislative requirements. A certificate of disposal must be obtained.
- The ICT Asset Register is updated to reflect the disposal of the asset
- Data Protection Act Compliance must be achieved for the disposal of all ICT equipment and software exit. To ensure compliance:
  - All media which held or may have held patient identifiable data or confidential or sensitive data must be wiped in accordance with the law and the prevailing Department of Health and Information Commissioner's Office requirements
  - All hard disks and any other media storage will be removed from the ICT equipment by the specialist supplier, in accordance with the terms of the contract.
- If removal is not practical, as a minimum standard, data shall be erased or overwritten to an approved standard, such as CESG; the UK Government's National Technical Authority for Information Assurance (IA)

6.7.5 Note that a wide variety of devices may contain media storage and be covered by this policy, including printers and photocopiers.

7 CYBER SECURITY

7.1 INTRODUCTION

7.1.1 **Cyber Security** is the protection of computer systems and the information that they hold from damage, disruption or interruption of the services that they provide. This is not about protecting computer systems per se but about protecting the processes and services that they provide and support.

7.1.2 The world of Cyber has its own language and there are a number of types of threat that exist as explained in Appendix 5 in addition to the general definitions in Appendix 1

7.1.3 There are a number of key roles in the Trust related to Cyber security:

- At Board level, the **SIRO** (Senior Information Risk Owner) is Simon Crawford, Director of Strategy and Deputy Chief Executive. The Deputy SIRO is the Head of Information Governance and is the Subject Matter Expert for IG.
- The Trust also has a **Caldicott Guardian**, Simon Gabe, a senior consultant in the Trust.
- The ICT department has a dedicated **ICT Security Manager** role. This role leads on all ICT Security matters and on the relevant standards within the IG Toolkit.
    - The senior ICT Managers for networks, servers and end user devices are also trained in security aspects of their specialist area.

7.1.4 The techniques for dealing with Cyber threats involve a three-fold approach:

- **Prevention**: ensuring that threats are prevented from having any impact on our systems and computers.
- **Detection**: detecting when a threat has not been prevented so that it can be dealt with appropriately before causing real damage.
- **Response**: resolving any threats that have materialised, minimising the impact and recovering the situation.

7.1.5 The objectives of the Security section of this Policy are to ensure that:

- Information is protected from unauthorised access, disclosure, modification or loss.
- Information and equipment are protected from accidental or malicious damage and theft.
- Safeguards to reduce all types of security risks are implemented at an acceptable cost.
- Audit records on the use of information are available as necessary.
- Information Governance (IG) Serious Incidents Requiring Investigation (SIRI) are properly identified, assessed, recorded and managed.

- All legal, regulatory and contractual requirements and standards of due care are met.

7.1.6 The Cyber Security standards in this policy support this approach and ensure that all staff are aware of their own role, and responsibility, to safeguards against these threats.

7.1.7 Some of the standards below apply to specific roles in the organisation including Information Asset Administrators (IAA) and technical staff within the IT department.

7.2 STANDARDS FOR USERS

7.2.1 All users of Trust systems and the IT infrastructure must ensure the safety and security of patient, staff and sensitive information at all times. There is legislation covering this area and to breach this legislation may cause the Trust to be liable to sanctions. A breach of these standards could cause damage to patients and will be subject to the Trust's disciplinary policy. The IT department will monitor usage of all Trust systems and use this information to help with any investigation into a potential breach of security.

7.2.2 There are a number of ways in which information can be compromised and other people could gain access to Trust systems and information on patients or staff. The standards in the previous sections of this policy all help protect information. In particular, the Acceptable Use and Access sections should be read by all end users of Trust systems.

7.2.3 All users of IT equipment and systems are required to report breaches or potential breaches (near misses) of security. This must be reported to the ICT Service Desk in the first instance.

7.2.4 The following standards must be followed by all users of Trust systems to help reduce the risk of this happening.

- Emails and other documents may contains links to websites or other external information. These can be sources of viruses or may contain inappropriate information. You must not click on such a link unless you know the sender of the email and are expecting a link to another site.
- Websites such as gambling or pornography may also contain viruses and other malicious software and should never be accessed from devices used for Trust business.
- You must not open or download files from unknown sources or that you are not expecting. Files are commonly used to spread computer viruses.

- Only encrypted removable/external media (USB sticks and external hard drives) being used for work purposes can be attached to a Trust device. This is not the best technique to transfer information and advice should be sought from the IG department if you need to transfer data. Such media should never be used for PID or sensitive information.
- You must never share your account details (user name and password) with another person (whether a Trust employee or not). If you do so then you will be held responsible for anything that they do on the Trust IT systems.
- Similarly, you must never write down your account details or make them easy to guess. This also opens up the Trust IT systems to unauthorised access.
- You must never leave a computer unattended so that other people can access your account. If the account is used in this way, with or without your permission, then all activity will be attributed to you and you will be held accountable for any breach of this policy.
- Whether using Trust-owned equipment or your personal equipment for Trust purposes, the equipment must not be left in an unsecure place. Such equipment should always be on your person, secure in your home or in a secure Trust location. The boot of your car is not secure and devices within it can be detected from the outside.
- When your device is not being used, it should be locked to avoid unauthorised use. An Inactivity timeout/password protected screensaver should be used.
- Do not store data locally on the Desktop or C drive.
- The loss of any equipment (including laptops, tablets and phones) must be reported to the Service Desk immediately.
- If the IT department recalls a device for maintenance/upgrade then this must be returned in a timely manner.

7.2.5 "Phishing" is a common technique used to try to get someone to click on a link or open a file from an email. The email may look like it is from a reputable source (e.g. a bank) and may say that your account has been hacked, for example. It will ask you to click on a link or open a file to enter information about you or your account. DO NOT DO SO. If in doubt, you must phone your bank separately and talk to them. Your bank will never ask for your PIN. You must forward any such emails to the Service Desk and delete them.

7.2.6 The standards in sections 7.3 to 7.10 inclusive are the responsibility of the IT department, Information Asset Administrators (IAA) and suppliers of IT systems. The subsequent sections do apply to staff.

7.3 END USER DEVICE SECURITY

7.3.1 This is the responsibility of the **Engineering Manager** working with the **ICT Security Manager.**

7.3.2 End User Device (EUD) Security centres on the desktop, laptop, tablet, Smartphone and printing devices used directly by Trust staff.

7.3.3 Security features, service levels, and management requirements of all EUDs will be identified and included in any specification for new devices.

7.3.4 The Engineering Manager will ensure that all EUDs conform to all relevant NHS Security Policies and standards.

7.3.5 Security features of End User Devices must include the following areas:

- A range of vulnerability detection/protection/response software such as Anti-virus to detect and respond to threats on the device.
- Port control to prevent the connection of unauthorised and unencrypted external devices
- Regular patching of devices to ensure operating systems and other core software is up-to-date
- Change of default admin usernames and passwords, and the regular change of admin passwords.
- Local admin rights should only be given to end users upon approval by the ICT Security Manager and should be avoided where possible.
- Prevention of locally-stored data (e.g. on Desktop or C drive)

7.3.6 An encryption solution must be deployed to protect all mobile devices (laptops, tablets, memory sticks and other removable or portable media).

7.3.7 Other static desktop devices, for example PCs, must be risk assessed and encryption or physical security applied if appropriate.

7.4 NETWORK SECURITY

7.4.1 This is the responsibility of the **Network Manager** working with the **ICT Security Manager.**

7.4.2 Network Security centres on the hardware and cabling infrastructure that provides Network connectivity for the organisation. This will include 'gateway elements' such as routers, switches, firewalls, external cabling, etc.

7.4.3 Security features, service levels, and management requirements of all Network services will be identified and included in any Network services agreement, whether these services are provided in-house or outsourced.

7.4.4 The ability of the Network service provider to manage agreed services in a secure way should be determined and regularly monitored, and the right to audit will be agreed.

7.4.5 The Network Manager will ensure that all connections to external Networks and systems conform to all relevant NHS Security Policies and standards, such as the Code of Connection and supporting guidance.

7.4.6 Security features of Network services must include the following areas:

- Firewalls to protect the Trust's network from external threats. These are to be placed at all borders with other Trust's/networks.
- Port control on the borders to allow traffic on defined communications channels only.
- Segregation of networks to allow the isolation of parts of the network.
- Regular patching of all network devices to ensure firmware and software is up-to-date
- Change of default admin usernames and passwords, and the regular change of admin passwords.
- Physically secure devices so that they cannot be physically manipulated (e.g. reset to factory default settings).

7.4.7 All Network connections and devices must be monitored for potential security breaches. All monitoring will comply with prescribed standards. Regular reports will be provided and circulated as necessary to ensure risks are assessed and addressed.

7.4.8 All Networks will be subject to regular Penetration Tests and the results reported to the relevant IT management group. The scope of such tests will be set by the ICT Security Manager.

7.5 DATA CENTRE/SERVER SECURITY

7.5.1 This is the responsibility of the **Data Centre/Server Manager** working with the **ICT Security Manager.**

7.5.2 Server security centres on the physical and virtual servers under the management of the IT department and housed in one of the Trust's Data Centres. Some servers in the Data Centre, and all off-site servers, are managed by third party companies.

7.5.3 Third party companies should be following best practice and conform to these standards. Their own security standards should be supplied and reviewed by the Server Manager and ICT Security Manager to ensure that this is the case.

7.5.4 The ability of a third party provider to manage servers in a secure way should be determined and regularly monitored, and the right to audit will be agreed.

7.5.5 Security features of servers must include the following areas:

- Anti-virus software installed to detect and respond to any threat on the server.
- Port control on the servers to prevent unauthorised attachment of external devices.
- Segregation of applications onto different servers (physical or virtual) to prevent a problem on one system affecting another.
- Regular patching of all servers (operating systems and other pre-requisite software) to ensure firmware and software is up-to-date

- Change of default admin usernames and passwords, and the regular change of admin passwords.
- Physically secure devices so that they cannot be physically manipulated (e.g. reset to factory default settings) and are inaccessible to unauthorised individuals.
- Administrator access to servers shall be restricted to a nominated and trained group of ICT professionals.
- Encryption is recommended in all cases where possible.

7.5.6 Similarly, the safety and security of the Data Centres must include:

- The Data Centre must by inaccessible by unauthorised individuals.
- Air conditioning controls must be sufficient to maintain the temperature at a safe operating temperature. There should be redundancy so that the loss of one conditioners does not affect the temperature.
- Power supply must be reliable and safeguarded from energy spikes and other supply problems.
- Uninterruptible power supplies (UPS) must maintain all critical systems in the event of a loss of external power supply to the Data Centre.
- UPS must be capable of triggering a shutdown of servers in the event of power loss.
- UPSs must be monitored and maintained to ensure their effectiveness.
- The cabling, power and devices within the Data Centre must be safe from flooding/leakage from the floor, walls or ceiling.

7.5.7 All servers must be monitored for potential security breaches. All monitoring will comply with prescribed standards. Regular reports will be provided and circulated as necessary to ensure risks are assessed and addressed.

7.5.8 All servers will be subject to regular security tests and the results reported to the relevant IT management group. The scope of such tests will be set by the ICT Security Manager.

7.6 THREAT DETECTION AND PREVENTION

7.6.1 A wide range of tools is available to help secure an IT network and devices. Some of the minimum standards have been detailed in the above section. There are other tools, detailed below, that should also be used to provide additional security.

7.6.2 By its nature, this list will be out-of-date before this policy is approved. Therefore, the ICT Security Manager has an ongoing responsibility to review the threat landscape and tools and should proposed changes on an ongoing basis.

7.6.3 Current best practice includes the following tools:

- Anti-virus at PC and server level
- Firewalls

- Encryption
- Port control on servers, network and end user devices
- Web filtering to prevent access to unauthorised sites
- Vulnerability scanning tools
- Intrusion Detection and Protection tools
- Monitoring/enforcement of password standards in network domain login and in systems

7.7 RESPONSIBILITIES OF THE INFORMATION ASSET ADMINISTRATOR

7.7.1 These responsibilities include giving access to systems, maintaining user accounts, configuring the system and performing system management/housekeeping duties. In this role, the IAA is professionally accountable to the Chief Information Officer (or delegated senior manager).

7.7.2 The form in Appendix 9 must be completed by the IAO/IAA for each system under their control/management.

7.7.3 Formal user access control procedures must be documented by the IAA, implemented and kept up to date for each system to ensure authorised user access and to prevent unauthorised access.

7.7.4 Processes must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access.

7.7.5 These processes will be subject to review and must be agreed by the Information Asset Owner (IAO). Each user must be allocated access rights and permissions to computer systems and data that: are commensurate with the tasks they are expected to perform (Position Based Access) and are commensurate with the data that they need access to (Workgroup Based Access).

7.7.6 For systems giving access to patient or staff information, training in that system must be given before access should be granted.

7.7.7 User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

7.7.8 Where group access rights are required to folders containing sensitive or confidential information, a nominated folder owner must be identified and each request for access must be authorised by the folder owner.

7.7.9 User names will be defined by the System Manager (IAA) of the system being accessed and will be unique. The preferred format, if the system allows it is XXX.

7.7.10 It is acknowledged that some systems may not support this approach and an alternative method may be used (e.g. employee number).

7.7.11 Generic (shared) user names are not allowed. The only exception to this is for generic network logons, which give Intranet access only. Any access beyond that (e.g. to another system) requires an individual logon.

7.7.12 Passwords will initially be assigned by the System Manager (IAA) of the system being accessed. It must be changed on first access by the user.

7.7.13 The IAA must use the configuration functionality of the system to define the standards for acceptable passwords. If the system allows it, the following standards should be configured and enforced:

- A minimum password length of 6 characters
- To contain at least one alphabetic character (a…z)
- To contain at least one numeric character (0…9)
- To contain at least one lower case and one upper case alphabetic character
- To prevent the user from repeating the same character more than twice in a row
- To force the password to be changed at every 60 days.
- To maintain a history of previous password and prevent a passwords from being repeated within 6 months of their first use.

7.7.14 The system should be configured so that after three successive failed attempts to log in, the account shall be disabled and an alert raised to the Information Asset Administrator (IAA). The IAA shall only reset the password after confirming the identity of the user. For some systems, this duty of the Information Administrator may be delegated to the ICT Service Desk by agreement and with appropriate training.

7.7.15 Where a Smart card is used to access a system (e.g. the eReferral System) then the Registration Authority process must be used as documented elsewhere.

7.7.16 System Management responsibilities include:

- Ensuring that the system runs well, reporting any issues to the supplier.
- Carrying out any “housekeeping” procedures such as deleting temporary files, monitoring log files, etc.
- Running and monitoring regular “jobs” such as reports
- Investigating any failed processes e.g. interfaces, reports, etc.
- Manage the supplier: their performance, issues resolution, escalation, deliverables, etc
- Schedule and test upgrades through liaison with the supplier and with Trust staff to minimise disruption and downtime.
- Maintain and manage any associated database (see below)
- Monitoring for any potential security breaches, including:
  - Multiple failed logons
  - Unauthorised access from third parties
  - Users attempting to access information for data not in their workgroup
  - Separation/segregation of duties issues (e.g. in the Finance system)

  - Unauthorised database level access
- For on-premise systems, working with the IT department to ensure that backups are taken regularly (in line with the RPO) and that restoring from backup is tested annually.

7.7.17 Configuration responsibilities include:

- Setting up new users, units, etc.
- Configuring the system for new forms, templates, screens, fields, workflow, etc.
- Ensuring the system matches the Trust set up e.g. organisational structure, etc.
- Configuring an inactivity timer on the system so that unattended operation locks the sessions without losing data. The timeout period should be agreed with the IAO. It should not be less than 10 minutes and should not be more than 30 minutes.

7.7.18 Training responsibilities include:

- Design and construct training courses and supporting material
- Maintain the system page on the Intranet (if applicable)
- Schedule training courses for new users, existing users, new functionality, system changes, etc.

7.7.19 Support responsibilities include:

- Help users understand and use the system.
- Managing user accounts (joiners, leavers, changers, passwords, etc).
- Investigate and resolve issues reported by users, escalating to others where necessary
- Ensuring that all licences are current and sufficient for the usage of the system. This includes any dependent software such as a database.

7.7.20 Supplier management responsibilities include:

- For hosted systems, ensuring that backups are taken regularly (in line with the RPO) and that restoring from backup is tested annually.
- Attending any recommended training courses ran by the supplier, covering the system management of the system.
- Maintaining the relationship with the supplier, holding regular service management meetings to ensure that the supplier is meeting the standards set out in the Service Level Agreement (SLA).
- Escalating any poor supplier performance to the IAO.
- Represent the Trust at User Group meetings

7.8 POSITION/WORKGROUP ACCESS

7.8.1 Where possible within a system access must be granted to only the functionality that a user needs and is authorised to use. This is known as position or role based access.

7.8.2 At the minimum, general users of a system should not have access to administration functionality.

7.8.3 The ability to reset passwords may be delegated to a discrete set of "super users" that have been specifically trained by the IAA.

7.8.4 The ability to carry out "back end" tasks (e.g. designing reports, configuring screens, etc) should be limited and not given to general users of the system.

7.8.5 For some systems, the professional standards of that function may dictate other rules. For example, for the Finance system, no one person is allowed to have both Accounts Payable and Accounts Receivable access.

7.8.6 Where possible within a system, access must be granted to only the information on patients or staff that a user needs to see (for example, if they deliver care to that patient). This is known as their workgroup.

7.8.7 This limitation may be to specific groups of patients (e.g. those in their caseload) or to a subset of information about that patient (e.g. ophthalmology not having access to chiropody).

7.8.8 On occasion or in specific teams (e.g. in A&E) a user should not be limited to the data that they can see.

7.8.9 Information that users view, change or add should be audited by the system so that the IAA can investigate any suspected breaches of confidentiality.

7.9 DATABASE SECURITY

7.9.1 Most systems have a database that stores the information used by the system. Common database systems are SQL and Oracle.

7.9.2 These database systems come with their own sets of utilities and management functions. It is the responsibility of the IAA to manage the database to ensure that the system's performance and security is maintained.

7.9.3 This responsibility may be delegated to a supplier (e.g. the supplier of the system that it uses) or other technical resource (known as the Database Administrator – DBA). However it is still the responsibility of the IAA to ensure that these activities are carried out and that any issues are reported through to the DBA.

7.9.4 The following minimum standards must be applied:

- Monitoring of database performance parameters including: available space, degree of fragmentation, degree of monitoring enabled, etc.
- Monitoring of log files on a daily basis for any issues that need resolving
- All direct database access accounts are protected from unauthorised access.
- Housekeeping activities are carried out on a regular (typically weekly) basis e.g. archiving of log files, ensure disk space is sufficient, etc.

7.9.5 The database software level must be maintained to the latest version that is supported by the system reliant on it.

7.9.6 If the database software level will become end-of-life and the system does not support a current version of the database software, then this should be risk assessed and escalated to the system supplier and IAO for resolution.

7.10 INACTIVITY

7.10.1 All systems should measure inactivity by the user and lock their session if it exceeds agreed parameters.

7.10.2 Inactivity can take place at two levels: the end user device and a system.

7.10.3 **For end user devices**:

- Desktops, laptops, tablets and Smartphones all have the ability to set timeouts for inactivity. Further to this, they can be configured to require a password or passcode to unlock.
- Trust-supplied devices will be pre-configured by the IT department with an inactivity timer of 5 minutes. After this time the Trust screensaver will appear.
- For user-supplied (BYOD) mobile devices accessing NHSMail, this functionality is automatically implemented on the device when the NHSMail account is added and is a pre-requisite of accessing NHSMail.
- For user-supplied (BYOD) devices not accessing NHSMail, but which do access other Trust systems, an inactivity time of 5 minutes must be setup by the user.

7.10.4 **For a system**:

- These standards apply to systems that hold patient or staff data, not to supporting systems such as Office products, dictation software, etc. It is recognised that not all systems have the capability to support these standards. Whatever functionality around inactivity timeouts needs to be reviewed and implement in discussion between the IAA and IAO.
- Locking the session on the system involves two stages:
- Stopping any more data entry or viewing of data unless the user re-enters their password to re-open the session.
- Disconnecting and terminating the user's session.

- In the first stage, no information previously entered may be lost.
- In the second stage any information entered that has not been committed to the system ("saved") will be lost.
- The IAA of the system should configure the timers for both stages. The timeout periods should be agreed with the IAO. The first stage should not be less than 10 minutes and the second stage should not exceed 45 minutes.

7.11 INCIDENT MANAGEMENT

7.11.1 An incident is defined as any issue or problem with IT equipment or systems that prevent the user from carrying out the normal duties of their job. Examples include:

- Unable to login to the device or system
- The device or system not functioning correctly, or as it has previously functioned
- A suspected breach of security of the device, system or information contained therein

7.11.2 A change request is defined as the situation where a device or system does function as expected but the user would like it to act differently. This may be a change in functionality or a change in use by the user.

7.11.3 All users of IT equipment and systems are required to report breaches or potential breaches (near misses) of security. This must be reported to the ICT Service Desk in the first instance. The reporting and management of incidents should take place according to the Incident Management Procedure.

7.11.4 All potential security breaches (near misses) must be investigated and reported to the IAO of the system and the ICT Security Manager. If the breach is deemed serious then it must be reported to the Head of Information Governance for investigation. The Head of IG will decide whether it needs reporting to the SIRO and national bodies in line with the standards in the IG Toolkit and NHS policy.

7.11.5 The management of all incidents, weaknesses and security related events will take into account the requirement, where necessary, to collect and preserve evidence to ensure compliance with any applicable legal requirements or disciplinary procedures. Where necessary external expert resources may be commissioned to support the collection and preservation of evidence.

7.11.6 Incident management comprises a number of stages:

- Prevention (auditing and monitoring)
- Identification
- Recording/reporting
- Evidence gathering
- Notifying
- Response

- Resolution

7.11.7 **Prevention** (Auditing and Monitoring)

7.11.8 The Trust's IT Infrastructure and systems shall be continually monitored by relevant tools available to the ICT Security Manager and other senior technical ICT staff. These will look for any suspicious activity occurring. This monitoring will enable the Information Asset Administrators (IAA) to identify any potential threats to the organisation's systems and enable a swift response to potential dangers.

7.11.9 Security weakness may be observed by anyone working on behalf of the Trust. Whilst weaknesses may not represent an incident, they should be reported for further investigation and remedial action as necessary. They should be reported to the ICT Service Desk, IAA and Information Governance team as soon as possible to prevent an incident occurring.

7.11.10 Staff should not attempt to prove that an observed system weakness can be exploited. Testing system weaknesses could be interpreted as potential misuse of the system and may cause an incident to occur.

7.11.11 Identification

7.11.12 There are several different types of system Security Incident that can lead to the loss of data (and/or system compromise) and therefore pose a risk to the integrity of systems.

7.11.13 Common examples of Security Incidents include:

- Deletion or damage/corruption of data
- System malfunctions or overloads – (may be an indicator of a security attack or breach)
- Inappropriate sharing of data
- Uncontrolled system changes – (Non-compliance with the Change section of this Policy)
- Software bug
- Access control violations – (Non-compliance with the Access section of this Policy)
- Theft or loss of an End User Device
- Breach of Physical Security of a server room, department, ward etc.
- Act of vandalism to Network cabling infrastructure on the external face of any building
- Inappropriate or accidental disclosure of user account details (password, username etc.)

7.11.14 Recording/reporting

7.11.15 Every incident, event or near miss must be recorded by reporting to the Service Desk and IAA. The information to be collected is detailed in Appendix 6

7.11.16 All staff should be aware that the earlier an actual or suspected security related incident is reported the more effectively it can be dealt with. Delay or failure to report an incident will often have greater repercussions for both users involved and the organisation itself.

7.11.17 Where incidents meet set criteria identified in the Trust's Risk and Assurance Framework, they shall be reported to the Head of Information Governance will shall report them to the SIRO ad CIO. A summary of the incident and its severity must be provided as a minimum with further details available upon request. Where incidents have involved PID (related to either patients or staff), the Caldicott Guardian must be consulted. The Head of IG and SIRO will determine whether the incident needs to be reported externally, using national guidance when determining the impact.

7.11.18 Evidence Gathering/Preservation

7.11.19 There are two primary categories of incident where the collection and preservation of evidence may be required. These are:

- Where internal HR disciplinary processes may be invoked
- Where the incident may lead to civil or criminal proceedings against the organisation or an individual

7.11.20 In both of these cases, the incident shall be classified as a Serious Untoward Incident (SUI) and the organisations Policy for handling SUIs shall also be invoked.

7.11.21 Consideration should be given in every incident investigation to the collection and preservation of original copies of any documents, material, software or ICT hardware, which may later be required or submitted as evidence.

7.11.22 During the course of any investigation if it becomes apparent that the matter could lead to legal proceedings, consideration should be given to requesting the assistance of the NHS Forensic Computing Unit. This team is part of the central NHS Counter Fraud and Security Management Services.

7.11.23 Notifications

7.11.24 These incidents will be reviewed by the ICT Security Manager on a regular basis to identify any underlying issues or risks. Any risks will be added to the relevant risk register with an associated action plan. This action plan will be signed off by the relevant IAO or SIRO, depending upon the impact.

7.11.25 A summary of all information security incidents will be provided to the SIRO on, at least, an annual basis alongside the ICT Risk Register. This is to ensure assurance is provided that the monitoring, escalation and management of security incidents is to the required standard. It is also an NHS requirement that the SIRO provides an annual summary report on reported incidents, which is included in the Statement of Internal Control.

7.11.26 Response and Resolution

7.11.27 The ICT departments Service Level Agreement (SLA) with the Trust shall set out the target response and resolution approach to incidents. The SLA shall include:

- The actions required of staff reporting the incident or event
- The ICT department obligations and response times
- The criteria for nominating an Incident Coordinator (if needed)
- The escalation and reporting requirements for the ICT Security Manager or nominated Incident Co-ordinator
- Criteria for declaring a near miss
- Criteria for a Serious Untoward Incident (SUI) and how to escalate in line with the SUI process
- The timescales for response and resolution

7.11.28 All procedures of security incident management should be reviewed by the Trust's senior ICT management team. It should be ensured that staff with responsibility for systems (IAAs) understand their responsibilities as set out in this Policy. This responsibility will include reporting and management of incidents that involve other organisations and service providers.

7.11.29 If the resolution of an incident results in a change to a system then this should be in compliance with the Change section of this Policy and documented accordingly.

8 GENERAL DATA PROTECTION REGULATION

8.1 INTRODUCTION

8.1.1 This section of the policy describes the standards to be followed that ensure that the Trust will comply with the **General Data Protection Regulation (GDPR)** which supersedes the **Data Protection Act** (DPA). It applies to all personal information held by or for the Trust in any format, including patients, relatives, carers and staff.

8.1.2 This policy applies to all staff employed by the Trust, including bank, agency and locum staff, students, voluntary staff, contractors and trainees on temporary placement.

8.1.3 The Trust is a public body and must comply with the principles and requirements of the General Data Protection Regulation (GDPR), which comes into effect from May 2018. Note that it applies to any organisation operating within the EU, regardless of whether the country involved is a member of the EU. Britain's membership (or not) of the EU is therefore irrelevant. GDPR replaces the Data Protection Act 1998 (DPA) which came into effect on 1st March 2000, replacing the Data Protection Act 1984 and the Access to Health Records Act 1990 (except in relation to the health records of people that have died).

8.1.4 This policy describes the principles of the GDPR, how the Trust applies them and the rights of patients and staff in relation to the Regulation. The GDPR includes many of the principles of the DPA but is more wide reaching. It also provides national regulators with new powers to fine organisations that breach the regulation.

8.1.5 The **Information Commissioner** (ICO), who maintains a register of notifications from all Data Controllers, oversees the provisions of the Act. A **Data Controller** is the person or corporate body who holds and directly controls the use and processing of the data. The Trust is a Data Controller. It is usually the "Data Processor" of it as well. For some outsourced systems, the Data Processor will be a different organisation.

8.1.6 The requirements of this policy and the Trust's legal GDPR duties will be overseen by the Trust's designated **Data Protection Officer** (i.e. role of Deputy Senior Information Risk Owner – Deputy SIRO held by the Head of Information Governance). The requirement for a **Privacy Officer** will also be fulfilled by the Deputy SIRO.

8.1.7 The Trust's **Information Governance Group** will oversee the arrangements for ensuring compliance with the requirements of the GDPR. This includes ensuring that all supporting Trust procedures are also updated as appropriate, maintaining an individual's right of access to their records. These procedures also define the activities of Subject Access Co-ordinators in supporting **Subject Access Requests** (SARs).

8.1.8 The Information Governance Group reports to the **Corporate Quality and Risk Committee**.

8.2 PRINCIPLES

8.2.1 **Principle 1 – transparency, fairness and lawfulness in the handling and use of personal data**. This means being clear with staff and patient about how their personal data will be used.

8.2.2 **Principle 2 – limiting the processing of personal data to specified, explicit and legitimate purposes.** This means not disclosing it or using it for purposes not originally intended.

8.2.3 **Principle 3 – minimising the collection and storage of personal data to that which is relevant and adequate for the original intended purpose.** Only collecting and storing the data that is need to fulfil the stated purpose.

8.2.4 **Principle 4 – ensuring the accuracy of personal data and allowing for it to be corrected or erased.** Taking steps to ensure the information we hold is accurate and can be corrected if there are any errors.

8.2.5 **Principle 5 – limiting the storage of personal data.** This includes only keeping it for as long as is needed.

8.2.6 **Principle 6 – ensuring the security, integrity and confidentiality of personal data.** Using appropriate measures to keep the information secure.

8.3 INFORMING PUBLIC AND PATIENTS

8.3.1 The Trust shall produce patient information leaflets and posters to make the general public and service users aware of why the Trust needs information about them, how this is used and to whom it may be disclosed.

8.3.2 These posters shall be placed in patient waiting areas and statements in patient handbooks, on survey forms, on research consent forms and verbally by those health care professionals providing care and treatment.

8.3.3 Leaflets (or appointment letters containing the information on the leaflets) will routinely be sent to all outpatients and made available to inpatients upon admission to hospital.

8.4 INFORMING STAFF

8.4.1 The Trust will deliver training to all staff in contact with patients or their information on the requirements of the GDPR and the need to maintain patient confidentiality.

8.4.2 Specific training shall be given to Subject Access Co-ordinators, who are likely to advise patients on issues relating to the GDPR or deal with applications for disclosure of information.

8.4.3 Guidance for staff is also available on the Intranet and within the NHS Confidentiality Code of Conduct, setting out when and how to inform patients about the holding, obtaining, recording, usage and sharing of their information.

8.4.4 Subject Access Co-ordinators will act as the point of contact for staff to refer to and to refer patients to for further assistance. They will also act as a point of contact for individuals to access directly to obtain further information on the GDPR.

8.5 REGISTRATION/NOTIFICATION

8.5.1 The Trust's Deputy SIRO is responsible for ensuring that the Trust registers annually with the Office of the Information Commissioner. This process is known as notification.

8.5.2 Failure to complete this process and keep the information up to date is a criminal offence. Notification is one means of ensuring the public are aware of the uses of their information by the Trust.

8.6 INDIVIDUALS RIGHTS – INCLUDING SUBJECT ACCESS/RIGHTS TO COMPLAIN

8.6.1 Trust policies ensure that the rights of individuals are upheld. Individuals have the following rights under the Regulation:

- Right of subject access to information held about them
- Right to prevent processing likely to cause harm
- Right to prevent processing for the purposes of direct-marketing
- Right in relation to automated decision-making
- Right to take action for compensation if the individual suffers damage
- Rights to take action to rectify, block, or destroy inaccurate data
- Right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the Regulation has been contravened

8.6.2 The Access to Health Records Act 1990 provides access rights relating to information about deceased patients' records.

8.7 DISPOSAL OF PERSONAL INFORMATION

8.7.1 It is important that personal information be disposed of in a secure manner.

8.7.2 It is essential that all paper waste containing personal information be confidentially disposed of according to relevant Trust Policies.

8.7.3 Reference is made to the Information Lifecycle Management Policy, the Confidentiality Code of Conduct, Health Records Policy, Corporate Records Policy and Information Security Policy.

8.7.4 For the disposal of entire systems, the Change section of this Policy should be followed.

8.8 TRANSFER OF PERSONAL INFORMATION OUTSIDE THE EUROPEAN ECONOMIC AREA

8.8.1 It is not envisaged that transfers of such nature will take place in the course of normal Trust business.

8.8.2 If such a requirement does arise it must take place with the suitable authority of the individual, if relevant, and also be agreed with the Trust's Deputy SIRO and/or Caldicott Guardian prior to transmission.

8.8.3 The Trust's Deputy SIRO is to be advised of any/all person-identifiable data flows outside of the UK (inbound or outbound).

8.8.4 Any and all transfers of PID must be in accordance with the Trust's Secure Data Transfer Procedure. Details of this Procedure are provided on the Intranet. Any data extracts including PID must be authorised by the responsible Line Manager for the relevant work area. Any bulk data extracts (i.e. 10 records or more) including person-identifiable data must be authorised by the responsible Director for the relevant work area and the Deputy SIRO (Head of IG).

8.9 PROCESS FOR COMPLIANCE WITH GDPR

8.9.1 Personal data must be processed lawfully at all times. Sensitive information that the Trust is not legally required to report to appropriate authorities, will only be shared with the consent of the individual.

8.9.2 Amongst the rights of the individual is the right to access the information held about them. A data subject must apply in writing (using the Trust's form available on the website) to gain access to a copy of the data held about them. A charge may be applied for the information supplied. However, there is no charge for access to view data.

8.9.3 The data subject may require clarification regarding any of the information recorded and a suitable member of staff, suitably qualified, will respond to any queries. This may include:

- A statement of whether there is any data held on the subject,
- A description of the data held, including copies if requested,
- An explanation of the uses the data is put to,
- An explanation of any information, codes, etc. that the data subject does not understand, and,
- When /whether the data may be disclosed.

8.9.4 The majority of requests for disclosure of personal information seek access to health records. A separate procedure exists for dealing with such applications (see Health Records Policy for details). This must be followed when such requests are made.

8.9.5 It is the responsibility of the Subject Access Request Officers to process and meet such requests. They shall also report on the number of requests received and on their performance against the statutory timescales for responding to them.

8.9.6 The Regulation also stipulates the need for a Data Protection Impact Assessment. This has been implemented in the NHS as a Privacy Impact Assessment (PIA). The standards in the New System section of this policy state the need for a PIA for new systems.

8.9.7 Another requirement is to map data across the organisation – whilst in transit between systems and at rest within a system.

8.10 PSEUDONYMISATION

8.10.1 Staff must only have access to the data that is necessary for the completion of the business activity that they are involved in. This applies to the use of PID for secondary or non-direct care purposes.

8.10.2 Pseudonymisation obscures PID items within a record sufficiently that the risk of identification of the individual is minimised to acceptable levels, thereby providing effective anonymisation. Pseudonymisation is a method that disguises the identity of patients by creating a pseudonym that may be used, by the “key holder” to re-identify an individual **if the need arises**.

8.10.3 This is different from anonymisation, which is a one-way process with no function to recover the identity of the person at a future time.

8.10.4 By using pseudonymisation, users are able to make use of patient data for a range of secondary purposes without having to access the identifiable data items.

8.10.5 Through implementation of Pseudonymisation, users are able to make use of patient-level data for a range of secondary purposes without having to access the identifiable data items.

8.10.6 Pseudonymisation can be achieved by

- Removing patient identifiers.
- Changing the way that an identifier is used: for example, using value ranges instead of instead of an absolute age.
- By using a pseudonym.

8.10.7 When pseudonymisation techniques are consistently applied, the same pseudonym may be provided for individual patients across different data sets and over time. This allows, if required, the linking of data sets and other information that is not available if the PID is removed completely.

8.10.8 All requests for access to patient and/or staff identifiable information for secondary use are to be processed in accordance with the Trust's Pseudonymisation Procedure, a copy of which is available via the intranet.

8.10.9 Any such requests for access must be authorised by the responsible Line Manager for the requesting work area.

8.10.10 Requests that would involve external transfer of person-identifiable data for secondary uses must also be authorised by the Trust's Caldicott Guardian and/or Deputy SIRO, after an initial assessment of the appropriateness of the request has been completed.

8.11 PROTECTING PID THROUGH A SAFE HAVEN

8.11.1 To aid compliance with this policy, and ensure restricted access to PID, person identifiable data must only be stored within a Safe Haven environment, with access restricted to a limited number of authorised staff.

8.11.2 A safe haven is a location, or in some cases a specific piece of equipment, which provides a safe location for the receipt of person confidential information.

8.11.3 Safe Haven Procedures must be used by Trust staff when they are sending or receiving PID and external organisations need to be assured that when they send PID to the Trust, they can be confident that they are being sent to a location that ensures the security of the data.

8.11.4 The Safe Haven Procedure is kept on the Trust Internet.

8.11.5 By using the Safe Haven procedures correctly, the Trust can demonstrate compliance with the relevant parts of the Data Protection Act and the Confidentiality: NHS Code of Practice.

8.11.6 Safe Havens must be located where large amounts of PID is being received, held or communicated.

8.11.7 Safe Havens must exist in the Trust to cater for all media types that may be used to send or receive person confidential information.

8.11.8 It is the responsibility of all staff to ensure that safe haven procedures are correctly used in all relevant instances of sharing PID.

9 FREEDOM OF INFORMATION

9.1 INTRODUCTION

9.1.1 This section of the policy describes the standards to be followed that ensure that the Trust will comply with the **Freedom of Information Act** (FOIA). It applies to all non-personal information held by or for the Trust in any format.

9.1.2 This policy applies to all staff employed by the Trust, including bank, agency and locum staff, students, voluntary staff, contractors and trainees on temporary placement.

9.1.3 The Trust is a public body and must comply with the principles and requirements of the Freedom of Information Act 2000 (FOIA). The FOIA, which came into effect on 1st January 2005 is part of the Government's commitment to greater openness in the public sector and replaces the non-statutory "Code of Practice and Openness in the NHS".

9.1.4 Under the Act, anybody may request information from a public authority that has functions in England, Wales and/or Northern Ireland. The Act confers two statutory rights on applicants:

- To be told whether or not the public authority holds that information; and if so,
- To have that information communicated to them.

9.1.5 This policy describes the principles of the FOIA, how the Trust applies them and the rights of patients and staff in relation to the Act.

9.1.6 The **Information Commissioner** (ICO) oversees the provisions of the Act.

9.1.7 The requirements of this policy and the Trust's legal FOIA duties will be overseen by the Trust's Deputy SIRO held by the Head of Information Governance. A **Freedom of Information Officer** is in place to provide administration of the Act.

9.1.8 The Trust's **Information Governance Group** will oversee the arrangements for ensuring compliance with the requirements of the FOIA. This includes ensuring that all supporting Trust procedures are also updated as appropriate, maintaining the public's right of access to information.

9.1.9 The Information Governance Group reports to the **Corporate Quality and Risk Committee**.

9.2 SCOPE

9.2.1 The Act applies to information recorded in any form. This includes:

- Information that is held electronically (such as an e-mail, information on a computer or an electronic records management system).
- Information that is recorded on paper (such as a letter, memorandum, reports, meeting agendas and minutes, or papers in a file).
- Sound and video recordings (such as a CD or video tape).
- Notes that have been written in the margins of a document, note pad or post-it note.

9.2.2 "Holding" information includes holding a copy of a record produced or supplied by someone else.

9.2.3 The Policy applies to all Trust employees, including bank and agency staff, and others conducting business on behalf of the Trust.

9.2.4 If the information requested is subject to a qualified exemption under Part II of the Act the Trust will implement the "public interest test" to determine whether the information can be released.

9.3 PRINCIPLES

9.3.1 The Policy supports the principle that openness and not secrecy should be the norm in public life. The Trust wants to create a climate of openness and dialogue with all stakeholders and improved access to information about the Trust will facilitate the development of such an environment.

9.3.2 The Trust affirms that individuals have a right to privacy and confidentiality through statutory provisions that prevent disclosure of identifiable information. The release of such information will be covered by the subject access provisions of the Data Protection Act 1998 and is dealt with in the above section of this Policy.

9.3.3 The Trust believes that public authorities should be allowed to discharge their functions effectively. This means that the Trust will use exemptions contained in the Act where absolute exemption applies or where a qualified exemption can reasonably be applied in terms of the public interest of disclosure.

9.4 RESPONSIBILITY AND CO-ORDINATION

9.4.1 The Deputy SIRO will act as the central point of expertise, guidance and advice for all complex and sensitive FOI requests, and the operation of this Policy, devolving management on a day-to-day basis as required.

9.4.2 The Deputy SIRO will manage the Trust's Freedom of Information Officer(s) for the processing of all complex or sensitive information requests.

9.4.3 The Deputy SIRO will:

- Ensure a consistent Trust position on potentially precedent setting cases.
- Provide guidance on all sensitive cases with a potentially high profile.
- Revise Trust guidance in the light of emerging case law and new policy.
- Be a source of expert advice and guidance within the Trust.
- Represent the Trust local, regional and national groups where Freedom of Information is discussed and decisions made

9.4.4 The FOI Officer will identify to the Deputy SIRO any "round robin" requests.

9.4.5 In exceptional circumstances, the Trust's Chief Executive will ultimately determine the disclosure of information and the utilisation of exemptions with the advice of the SIRO and appointed Solicitors, as appropriate.

9.5 RIGHT OF ACCESS & EXEMPTIONS

9.5.1 The Act provides a general right of access to information held by the Trust subject to certain exemptions and conditions contained in the Act. There are two aspects to this general right of access:

- The right to be told whether or not the public authority holds the information of the description specified in the request (referred to as the 'duty to confirm or deny').
- If that is the case, to have the information communicated provided that it may be disclosed.

9.5.2 The Trust's 'duty to confirm or deny' is retrospective in that if the Trust holds the information it must provide it, subject to certain exemptions and conditions.

9.5.3 Under section 1(3) of the Act, the 'duty to confirm or deny' does not arise where the Trust:

- Reasonably requires further information in order to identify and locate the information requested
- Has informed the applicant of that requirement.

9.5.4 In these circumstances, the Trust will make reasonable efforts to contact the applicant for additional information pursuant to their request, should further information be required.

9.5.5 Under section 2 of the Act the Trust may not have to comply with the 'duty to confirm or deny' if the information is exempt under the provisions of Part II of the Act. These provisions confer either an absolute exemption or a qualified exemption.

- An absolute exemption will be applied if the information requested falls into the category of information so exempted through section 2(3) of the Act.

- A qualified exemption may be applied if in all the circumstances of the case, the public interest in maintaining the exclusion of the 'duty to confirm or deny' outweighs the public interest in disclosing whether the Trust holds the information. The Trust will seek to use the qualified exemptions sparingly and will, in accordance with section 17 of the Act, justify the use of such exemptions.

9.6 VEXATIOUS OR REPEATED REQUESTS

9.6.1 The Act provides that the Trust is not obliged to comply with a request for information if the request is vexatious. "Vexatious" has been defined in this context as "manifestly unjustified, inappropriate or improper use"".

9.6.2 Where the Trust has previously complied with a request for information made by an identifiable applicant, it is not obliged to comply with a subsequent identical or similar request from that applicant unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request.

9.6.3 The Deputy SIRO will advise the Trust's Freedom of Information Officer in determining whether a request is vexatious, which may require advice from the Trust solicitor.

9.7 VALID REQUEST

9.7.1 The standards in this section of the Policy only apply to 'valid' requests. To be valid the request must satisfy all of the following:

- The request is in writing.
- The request provides the name of the applicant and a return address.
- The request adequately describes the information that is required.

9.7.2 Where a person is unable to frame their request in writing the Trust will ensure that appropriate assistance is provided to enable that person to make a valid request for information.

9.7.3 A valid request may be received by any employee of the Trust. Upon receipt, a valid request must be forwarded immediately to the Trust's Freedom of Information Officer.

9.8 FEES AND CHARGES

9.8.1 The Act provides that the Trust is not required to comply with expensive requests. The Statutory Instrument 2004 No. 3244 – The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004 sets the appropriate limit for the Trust.

9.8.2 Therefore, if it would cost more than the limit for the Trust to respond to a request, the Trust need not comply with it. The limit covers the time taken to search, retrieve, print, copy and extract the information. It does not cover the time taken to consider whether an exemption applies, carry out any redaction or consideration of the public interest test.

9.8.3 Complying with requests which would cost more than this ceiling will be determined by the Deputy SIRO. For requests that would cost less than the ceiling, no standard fee will be charged, but a charge for the full cost of disbursements (photocopying, printing and posting) may be levied.

9.8.4 Full cost of disbursements may be levied at the discretion of the Trust on a case-by-case basis. Full cost of disbursements will only be levied if the following are satisfied:

- The full cost of disbursement is greater than £50 (where an A4 photo-copy/ print out is 10 pence per page); and
- The full cost of disbursement total is known at the time the initial access to information request is considered by the Trust.

9.9 CONSULTATION WITH THIRD PARTIES

9.9.1 The Trust recognises that there may be circumstances in which access to information requests may relate to persons other than the applicant and the Trust; or where disclosure of information is likely to affect the interests of persons other than the applicant or the Trust.

9.9.2 In such cases, the Trust will advise third parties of the Trust's duty to comply with the Act, and information will be disclosed unless an exemption applies. The Trust may consult with third parties to determine whether the 'duty to confirm or deny' arises or whether or not an exemption applies.

10 BRING YOUR OWN DEVICE (BYOD)

10.1 INTRODUCTION

10.1.1 The standards in this section apply for the situation where a member of staff's is using their own equipment for work purposes. This is known as **BYOD** (Bring Your Own Device).

10.1.2 The Trust may allow BYOD to be used to access specific systems (for example, NHSMail) due to the increased mobility of the modern workforce. This in turn ensures that there is a resulting increase in user satisfaction/productivity and may also help to reduce capital expenditure on ICT end user devices.

10.1.3 However, there is still a requirement to meet strict standards of security, access control and acceptable use as dictated by other sections of this Policy. For the avoidance of doubt, all sections of this policy apply regardless of ownership of the device being used to access Trust systems and information.

10.1.4 The following sections outline the types of devices, standards and constraints of using personal devices for work purposes.

10.2 DEVICE TYPES

10.2.1 Due to the constant changing and release of devices and operating systems, this policy cannot stipulate exactly which are usable on a BYOD basis. The ICT department will therefore consider which devices and minimum Operating System level are able to be used by individuals for work purposes and keep a list separately.

10.2.2 This list must be maintained regularly to reflect any developments in device technology or updates/changes by the device owners.

10.2.3 Acceptable devices shall be limited to the following types:

- Non-Smartphones (for phone and SMS use only).
- Smartphones (for phone, SMS, email, Internet, "app" and other uses)
  - Android
  - iOS
- Tablets
  - Android
  - iOS
  - Windows
- Laptops: Windows
- Desktop PCs: Windows (home-based)

10.2.4 Operating System version for each device must be at the latest released by the supplier within 3 months of that release. This will ensure appropriate levels of security and that devices have fixes to known bugs.

10.3 SECURITY STANDARDS

10.3.1 The device must conform to the prescribed standards in the Security section of this Policy, including:

- Technology applied for security, such as anti-virus software (where the device is able to support this), authentication and encryption.
- Mobile device controls such as PIN requirement, encryption, remote wipe, GPS tracking, etc.

10.3.2 Users of personal devices will be required to follow the requirements of the Trust's password procedures which will dictate the need for a complex password attached to their devices at all times.

10.3.3 Use of email in support of Trust business shall be conducted using NHSMail only. Personal email systems shall not be used for work purposes.

10.3.4 Staff using their own laptops, tablets or smartphones for business purposes shall not store or cache data locally. The laptop, tablet, smartphone or netbook may act only as an interface allowing a user to work with the organisation's information.

10.3.5 Users of personal devices must adhere to the Acceptable Use section of this policy, which prohibits the access of sites known for spreading malware, such as pornography and gambling.

10.3.6 The Trust will deploy its own Mobile Device Management (MDM) app to the device so that its security can be guaranteed.

10.4 SUPPORT

10.4.1 Reimbursement for the cost of usage of the device will be subject to the Trust's expenses policy.

10.4.2 The ICT Service Desk will provide support for personal devices on a best endeavours basis only and such support will be limited to the business use of the device only.

10.5 DATA OWNERSHIP

10.5.1 Any Trust data held on a non-organisation owned device will remain the sole property of the organisation.

10.5.2 The Trust reserves the right to carry out any actions required on the individual's personal device necessary to process or safeguard that data including, for example, a remote wipe of the data if the device is lost or stolen.

10.5.3 It is the individual's responsibility to back up their own personal data on their device (including photos, contacts and text messages) and the organisation does not accept responsibility for the loss of such data in the event of a remote wipe being necessary.

10.6 APPS

10.6.1 Devices, for example iPhones and iPads, must not be "jail broken" or "rooted" to reduce the risk of installing non-manufacturer vetted operating systems and applications.

10.6.2 Users should avoid sites or applications that rely on a heavy use of Flash Player as this is often a route in for malware.

10.7 EXIT

10.7.1 On leaving employment with the organisation, the ICT Service Desk must be notified so that access from the network and systems can be removed.

10.7.2 All personal devices that have been used for work purposes will have to be subjected to a cleansing process involving the removal of:

- Access tokens
- Email access
- Organisation-owned data
- Applications installed to support access to Trust systems (including management tools).

11 EMERGENCY PLANNING AND DISASTER RECOVERY

11.1 INTRODUCTION

11.1.1 ICT disasters happen. There come in many shapes and forms, from Cyber-attacks to the failure of equipment. It is therefore essential that plans are in place so that Trust services can continue in the event of a disaster.

11.1.2 **Disaster recovery** is the term given to the steps to recover from a disaster. For ICT disasters, this is the responsibility of the IT department, IAA and appropriate suppliers.

11.1.3 **Business Continuity** is the term given to the steps to continue running Trust services whilst a disaster is being recovered from. This is the responsibility of each department affected with the assistance of the IAA.

11.1.4 It is the responsibility of local departments to develop their own local procedures so that they can capture data and continue to operate during an ICT disaster situation. The ICT department's responsibility is to minimise the likelihood and impact of a disaster and to recover from it.

11.1.5 Key risks to critical ICT functions, which would result in the loss of ICT services or data, should be identified and documented in the ICT Risk Register in line with the Risk and Assurance Framework and in discussion with key stakeholders.

11.1.6 It is not expected that the ICT department will have the ability to continue to deliver all ICT services at usual service levels in the event of an emergency; some critical functions may need to be scaled up, while others may need to be scaled down or suspended.

11.1.7 An assessment of the resilience and redundancy of the ICT Infrastructure and systems will be undertaken to formulate appropriate strategies for Emergency Planning.

11.1.8 The disaster recovery of Systems hosted outside of the Trust, or hosted inside but managed by an external supplier, is the responsibility of the supplier. The ICT department will give assistance where possible, particularly to test recovery or to provide connectivity to the system.

11.2 STAGES IN A DISASTER

11.2.1 There are a number of stages in a disaster situation and the plans and activities need to consider each of these stages.

11.2.2 **Pre-disaster** is before a disaster has occurred. It consists of "Business as Usual" activities and these must include tasks that would help the Trust mitigate the impact of a disaster or to reduce how long it lasts. These activities include:

- For the IT department:
  - Ensuring that the infrastructure is as robust and resilient as appropriate.
  - Ensuring that backups are taken on a regular and frequent basis.
  - Having contracts in place with third party companies so that damaged or faulty equipment can be replaced quickly.
  - Working with suppliers to ensure that support levels and the infrastructure of systems that they manage is sufficient to meet the needs of the Trust.
- For Trust services and departments:
  - Having documented processes to follow in the event of a disaster.
  - Having contracts in place with third party companies so that damaged or faulty equipment can be replaced quickly.
  - Ensuring that staff are trained in "downtime" procedures.
  - Considering activities such as printing out clinic lists before the clinic starts.

11.2.3 **Disaster** period is when the disaster is actually occurring. During this time, the Trust initially has to detect that a disaster has occurred and understand the nature of it so that appropriate decisions can be made with regard recovering from it. This may involve isolating or shutting down systems or escalating problems to suppliers. The IT department must be focused on this and the Trust services must be focused on continuing to provide services or on communicating how they are affected.

11.2.4 **Recovery** period is when the IT department (for an IT disaster) is focused on recovering from the disaster. This may involve rebuilding systems/servers or virus checking them; it may involve purchasing new equipment or moving equipment to another site. Trust services affected must continue to run downtime procedures. They will be given an indication as to when the IT systems will be "up" again and therefore should start to prepare for the next stage.

11.2.5 **BAU.** Business as Usual will return. For IT, this stage must include analysing the disaster, understanding the root causes and deciding on any changes needed in the future to mitigate against a similar disaster in the future. For Trust services activities must focus on both continuing to run services and on ensuring that all services that operated during the previous stages have been fully delivered and that necessary information is retrospectively entered into Trust systems.

11.3 COMMUNICATIONS

11.3.1 A Communications Plan must be developed to support the Emergency Planning processes. The precise details of the communications plan are likely to evolve alongside the management of the incident; but the general principles to be followed are detailed here.

11.3.2 Identify **who** needs to be consulted with and who needs to be informed; the former implies a more active relationship (e.g. this may be a key supplier or internal customer) while the latter may be the general "all user" staff population. Other Trusts may also be affected by loss of our ICT systems and should also be included in the comms plan.

11.3.3 Identify **when** to communicate; this is likely to be at the point of invocation and at key points whilst the plan is active.

11.3.4 Identify **how** to communicate; this may be affected by the nature or source of the incident (e.g. email system is down) so judgement will have to be used as to the most effective and efficient way of letting others know that the DR plan has been invoked. Contact Details should be documented and include all possible means of reaching key individuals so as to provide alternative communication opportunities.

11.3.5 Identify **what** to communicate; depending on the incident, it may be possible to provide detailed updates or it may be more feasible to provide summary details. Consult with the Communications team to support you when making these decisions.

11.4 ICT INFRASTRUCTURE RESILIENCE AND REDUNDANCY

11.4.1 The ICT department, and relevant suppliers, are responsible for ensuring an appropriate level of resilience and redundancy of the ICT Infrastructure in order to minimise the likelihood and impact of a disaster causing any loss of systems or access to data.

11.4.2 The order of recovery of infrastructure and systems will depend on the actual circumstances of the disaster and which systems, or ICT components, are affected. Until this is known, the following priorities must be assumed:

11.4.3 Priority One

- Core network infrastructure (links, switches, hubs) – to establish the capability to provide service at and between sites.
- PSTN and IP telephony systems – to provide voice connectivity with other sites and agencies.
- Network management infrastructure – to provide the capability to test, view and control the status of the core network.
- Core servers providing domain logon to staff.

- End user device management utilities – so that any changes necessary to the end user devices can be managed and deployed centrally. This also include anti-virus software management tools.

11.4.4 Priority Two

- Systems providing access to patient information (PAS, Symphony, Pharmacy, etc) and to staff availability (rostering, ESR, etc)
- e-Mail systems – to enable communication to other sites and agencies
- File and print services – to provide access to user files and shared folders

11.4.5 Priority Three

- External networks – connectivity to N3 (and hence the Internet) and any other external networks.
- Other systems (e.g. occupational health, finance etc).

11.5 DATA RESILIENCE AND REDUNDANCY

11.5.1 The **Recovery Point Objective** (RPO) must be defined by the IAO for each system. This is the maximum acceptable level of data loss following a disaster that could be suffered without severely affecting patient care. The RPO represents the point in time, prior to the disaster, to which lost data can be recovered (given the most recent backup copy of the data).

11.5.2 In most circumstances, the RPO will be one day or more. This will support the use of traditional daily backup technology to recover data up to one day old. An RPO of less than one day would call for different resilience/redundancy technology (e.g. mirrored storage on another site) which would require a business case to justify.

11.5.3 For systems hosted and managed by the ICT department, it is their responsibility to implement and manage the technology that will enable the chosen RPO.

11.6 DATA RECOVERY

11.6.1 The **Recovery Time Objective** (RTO) is the period of time within which business and/or technology capabilities must be restored following a disaster. This is the acceptable amount of time following a disaster that can be passed before severely affecting patient care.

11.6.2 In most circumstances, the RTO will be three days or more. This will support the recovery activities and resource levels of the ICT department and suppliers. An RTO of less than three days would call for different levels of support and equipment to be needed (e.g. spare servers ready to go).

11.6.3 For systems hosted and managed by the ICT department, it is their responsibility to implement and manage the technology that will enable the chosen RTO.

11.6.4 The organisation's decision on the timescale for the RTO is relative to the extent to which the interruption disrupts normal business operations and increases the exposure to risk. The risk scoring will be calculated in accordance with the organisation's Risk and Assurance Framework

11.6.5 The **Maximum Tolerable Period of Disruption** (MTPD) is the timeframe within which a recovery effort must succeed before the service fails, the 'worst case scenario'. If this time point is reached or exceeded, the likelihood of any recovery is greatly reduced. The RTO must be shorter than the MTPD, with the RTO acting as a benchmark to assess progress with and likely success of a full recovery before the MTPD is reached.

12 PROCESS FOR IMPLEMENTATION OF POLICY

12.1 INTRODUCTION

12.1.1 Implementing this policy involves the following activities:

- Consulting sufficiently amongst the IT department and key system owners (IAOs) to ensure it consider all viewpoints and is approved by appropriate groups.
- Communicating it to all relevant staff, including training where necessary.
- Agreeing Key Performance Indicators that align with the standards within this policy
- Monitor these KPIs as evidence that the policy is being followed.
- Regularly review the policy and the standards within it to ensure that they are appropriate for the Trust and comply with best practice or changing circumstances.

12.2 TRAINING AND COMMUNICATION

12.2.1 Once approved, this policy will be communicated Trust-wide through the following channels:

- The daily email bulletin to all staff
- The Intranet
- Tabling at appropriate groups and committees
- Cascading through management line
- Through the ICT Service Desk system ("Top Desk")

12.2.2 The Information Asset Administrator network needs to be introduced with regular meetings, professional accountability to the CIO and training in their responsibilities. Gaps in IAA resources need to be escalated to the IAO for resolving.

12.3 KEY PERFORMANCE INDICATORS

12.3.1 The Key Performance Indicators are detailed in Appendix 7 These are designed to demonstrate that each element of this policy is being implemented and followed.

12.3.2 These shall be reviewed at least annually. A change to the KPIs in the Appendix does not require a re-approval or ratification of this policy.

12.4 MONITORING ARRANGEMENTS

12.4.1 The success of this policy is measured through the KPIs. These should be reported at the ICT Strategy Group meetings and monitored there. Any changes to the policy or actions needed to improve the success of the policy will be agreed by the group and acted upon.

12.5 REVIEWING ARRANGEMENTS

12.5.1 This policy should be reviewed every two years.

12.5.2 The appendices should be updated/reissued on a regular basis to reflect new information. This shall not require a re-approval or ratification of the policy.

APPENDIX 1 DEFINITIONS AND GLOSSARY

The following terms are used in this report and defined here.

- **Staff/user:** general term for a user of Trust IT services. This includes anyone using equipment to access Trust information including members of staff, volunteers, students, visitors, contractors and suppliers. The term "staff" is not used to imply an employment contract with the Trust.

- **Digital:** General term used to cover all areas of the directorate headed by the Chief Information Officer. The directorate covers the ICT, Systems, IG and Medical Records departments. Medical Records policies are outside of the scope of this digital Policy.

- **ICT:** Information and Communication Technology department. This department is responsible for the procurement, installation, operational management and support of the Trust's entire IT infrastructure. This comprises hardware and software for networks, servers, data centre and end user devices.

- **Systems:** This department is responsible for the procurement, implementation, operational management, support and training for major clinical software used across the Trust. This includes SystmOne, PAS, ePro, GCIS, eRS and the Clinical Portal.

- **IG:** Information Governance. This department leads on ensuring that the Trust is compliant with relevant legislation including the Data Protection Act, Freedom of Information and the standards within the NHS Information Governance Toolkit.

- **Network:** The Trust's ICT Network is the collection of devices and wires that provide connectivity from an end user device to the system or data that they wish to access. This system could be on the same Trust site as them, a different Trust site or on the Internet (anywhere in the world). Connectivity could be wired or wireless.

- **LAN:** Local Area Network: the network within a single site extending from a Data Centre or other communications room to the end user devices. This can be wired (Ethernet cables with patching) or wireless (Wi-Fi).

- **WAN:** Wide Area Network: the network that joins sites together to allow communication between them. The Trust has a WAN that connects all 40+ sites and also has connections to the outside world (N3/HSCN and the Internet).

- **N3/HSCN:** The NHS-wide WAN is known as N3 (in the process of being replaced with HSCN) and connects all NHS Trusts together aiding communication between them. Each Trust has one of more connections from its WAN to the N3 network.

- **Server:** large computer (or group of computers) which hosts major systems, stores files or aids the management of the whole IT estate. Servers are housed in a secure location with environmental controls and physical security.

- **Data Centre:** room used to house servers securely and in safe environmental conditions. The Trust has three data centres across Northwick Park Hospital and Ealing Hospital sites. Some systems (e.g. SystmOne) are housed in a supplier's data centre, not the Trust's one.

- **End User Device:** device used by end users to access files, systems and other information. Types of end user device include desktop PC, laptop PC, tablet and smartphone. Other end user devices may include printers, display screens, projectors, etc.

- **BYOD:** Bring Your Own Device: the term used for when staff wish to use their own end user devices (usually tablet or smartphone) for work purposes.

- **PID:** Person/Patient Identifiable Data. Any data that can identify an individual because of the way in which the information has been collated, the context in which it is or may be used, or as a result of combining it with other information already held. This includes personal information (such as name, address, date of birth, NHS number) as well as sensitive information (such as religion, sexual preference, union membership, political views and any information regarding the physical or mental health of the person). It applies to both patients and staff.

- **GDPR**: General Data Protection Regulation. Legislation that protects the rights of an individual in terms of the security of data held on them. It also gives them right to access the data and puts a responsibility on the Trust to ensure compliance. Supersedes the DPA.

- **DPA:** Data Protection Act. Forerunner to the GDPR.

- **FOI:** Freedom of Information Act. Legislation that gives an individual the right to request and obtain information from the Trust that relates to non-PID e.g. how the Trust operates, general statistics, etc. The legislation states time limits by which the Trust must respond.

- **IGT:** Information Governance Toolkit. Set of standards across the NHS that help ensure compliance with the GDPR/DPA, FOI and other best practice across how information is managed. Trusts must score an average level of 2 (out of 3) across the relevant standards to be deemed "satisfactory" in their compliance.

- **IAO:** Information Asset Owner. The "business owner" of a system ultimately responsible for its specification, procurement and operation. With the exception of some Trust-wide systems, the IAO should not be a member of the IT directorate.

- **IAA:** Information Asset Administrator. The "system manager" of a system responsible for day-to-day operational management of a system including configuration, support and training of users. The IAA may not be full-time and may sit within IT or within another Trust department, but for their IAA duties should have professional accountability to the CIO.

- **SLSP:** System Level Security Policy. Document which describes the various roles, responsibilities and features related to security for a system.

- **PIA:** Privacy Impact Assessment. Describes and assesses the impact on patient confidentiality of a system, or changes to it. This will include how the data is stored and any potential risk of a future breach of confidentiality.

- **Cyber Security:** Cyber Security is the protection of computer systems and the information that they hold from damage, disruption or interruption of the services that they provide.

- **User name:** Unique identification given to a member of staff so that they can log in to a system. Different systems have different rules or formats for user names and therefore a user may have different user names for different systems.

- **Generic user name:** this is a non-unique user name at a PC level only, shared by a number of users. This allows limited access to IT services. Typically, this gives access to the Trust's Intranet only. Onward access to other systems (e.g. the Clinical Portal, NHSMail) requires a system-specific user name and password unique to the user.

- **Password:** A word, phrase or collection of symbols that should be known only to the individual and which, together with their unique user name, gives them access to a system.

- **Biometric:** A physical property of an individual which is unique to them and can be used (in addition to or as an alternative to their password) to access a system. Common biometrics include fingerprints, iris and facial recognition.

- **Smartcard:** Credit card sized device used, along with a password, to access some systems (e.g. electronic Referral System).

- **Policy:** A policy is a statement of intent that is adopted and followed across the Trust. Policies direct Trust practice in fulfilling statutory and organisational responsibilities. They clarify roles, relationships and responsibilities and can serve as a basis for decision-making in any given scenario.

- **Procedure:** A procedure translates policies into action: i.e. they are practical ways of accomplishing a task or goal – often by following a series of 'how to' steps in a regular, definite order. Procedures 'provide the information to carry out the intent' defined by a policy.

APPENDIX 2 EMAIL BEST PRACTICE

- **DO:**
  - View your Inbox regularly and respond to requests promptly
  - Advise people when you are not available to view incoming mail. When out of the office, use the 'out of office assistant' tool within MS Outlook or NHSMail to notify others, and explain if mail is being forwarded to somebody else in your absence
  - Be careful when selecting who receives your e-mails, especially when using "Reply to All". Ask yourself "Do all recipients need to see the reply?"
  - Use distribution lists with care – is it important that all addressees receive this email?
  - Check the full email trail to ensure that it is all relevant to the latest email. Edit and remove older emails in the trail if not relevant.
  - Check the e-mail before pressing "Send". In the event of a mistake, use the tool within your system to "recall" the message. Note: you can only recall unread messages
  - Use discretion when forwarding a long e-mail message to group addresses or distribution lists
  - Place large attachments in a shared location (where possible) and then send the path to the file via the e-mail (so as not to overload the network)
  - Use discretion with read receipts
  - Use the subject field with a few short descriptive words to indicate the contents of the message. It will assist the recipient in prioritising opening of messages and aids future retrieval of opened messages
  - Type your messages in a mixture of upper and lower case – using just CAPITAL LETTERS can be considered aggressive
  - Use the BCC field if you are sending the email to a large number of people, particularly if they are outside of the Trust.
- **DO NOT:**
  - Use patient-identifiable information within internal e-mails – however, if it is necessary then use local ID numbers (or preferably the NHS Number), along with 'date of birth' or similar secondary identifier, to ensure the individual is uniquely identified.
  - Send to external email accounts any patient identifiable information except under the conditions listed in this policy. If you are unsure of whether or not an external email destination is permissible to send identifiable information to, you must contact IG or the ICT Service Desk.
  - Send person identifiable clinical correspondence direct to a patient's personal e-mail account unless there is a clearly documented consent received on behalf the patient
  - Use other people's mail accounts to send your e-mails.
  - Send e-mail that may be misconstrued or cause offence to others.

- Send mass mailing circulars via e-mail unless it is to the clear business benefit of the Trust. If this is necessary do not use the TO or CC field for the recipients.
- Send to too many people, just because you can!
- Send large groups of attachments by e-mail as they can cause network congestion.
- Send computer programme files as attachments, unless absolutely essential.
- Give others authority to view/amend your mailbox unless fully justified.
- The use of colloquial language is considered unsuitable for e-mail and should be avoided. Witty comments, whilst appearing harmless to the sender, may be considered offensive to others and should also be avoided.
- Make comments in messages that may be considered defamatory or may cause false rumours.
- Use offensive, sexist or racist comments in e-mail under any circumstances. Violation is likely to result in disciplinary action, including dismissal, and could lead to prosecution under current legislation.
- Send messages containing “fancy” fonts or colour schemes as they can sometimes be difficult to read or print out. Stick to a plain font, such as Arial, and to the default colour scheme of your e-mail system.

APPENDIX 3 NEW SYSTEM FORM

- Request form to support the introduction of a new system.

Title:		**Date**:	
Description of system:			
Submitted by:		**Dept.:**	
Current system used for this purpose:			
Why is this system not suitable:			
Outline Business Case:	Yes/No	**Approved date**:	
Specification:	Yes/No	**Completed date:**	
Procurement:	Yes/No	**Completed date:**	
Full Business Case:	Yes/No	**Approved date**:	
PID:	Yes/No	**Project Board**:	Yes/No
PIA:	Yes/No	**SLSP**:	Yes/No
Legacy system to be disposed:			
IAO:		**IAA**:	

APPENDIX 4 SYSTEM CHANGE FORM

- Request form to support changes to a system or infrastructure component.

Title:		**Date**:	
Description of change request:			
Submitted by:		**Dept.:**	
Emergency change request?		Yes/No	
Reason for change:			
Business Case:	Yes/No	**Approved date**:	
Change specified:	Yes/No	**Completed date:**	
Procurement:	Yes/No	**Completed date:**	
Change approved:	Yes/No	**Approved date**:	
PID:	Yes/No	**Project Board**:	Yes/No
PIA changes:	Yes/No	**SLSP changes**:	Yes/No
Legacy system to be disposed:			
IAO:		**IAA**:	

APPENDIX 5 TYPES OF CYBER THREATS

The following table defines some of the types of threats and other terms used in the world of Cyber Security.

Term	Definition
Malware	General term for malicious software that is specifically designed to disrupt or damage a computer system.
Trojan Malware	Software that contains other malware inside it – so the first piece of software does not look malicious but it later releases a more malicious program.
Ransomware	A type of malware designed to block access to a computer system or stored information until a sum of money is paid. This is typically achieved through encrypting the hard disk and only releasing the key when the ransom is paid.
Malvertising	The use of online advertising to spread malware. Malvertising involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages.
Vulnerability	Flaw in a system that can leave it open to attack. A vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat.
Exploit kits	Exploit kits or exploit packs refer to a type of hacking toolkit that cybercriminals use to take advantage of vulnerabilities in systems/devices so they can distribute malware or do other malicious activities.
Patch	A patch is a piece of software designed to update a computer program or its supporting data, to fix or improve it. This includes fixing security vulnerabilities and other bugs, with such patches usually called bug fixes or maintenance releases, and improving the usability or performance.
Phishing	Is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. The recipient is coaxed to click on a link that takes them to a website that may look authentic. They are then prompted to entered confidential information that can be used to obtain money, or information from

Term	Definition
	them.
Remote code execution	The ability to trigger malicious code execution from one machine on another (especially via a wide-area network such as the Internet)
Anti-virus	Software on a computer that detects malware and isolates it to protect the computer.
Anti-spam	Software that intercepts emails which may contain phishing or similar threats.
Web filtering	A utility that stops people accessing websites that are banned as being inappropriate or malicious.
Intrusion Detection	Detecting where and when an attempt to access systems is taking place.
Intrusion Prevention	Preventing attacks to systems and the infrastructure

APPENDIX 6 INCIDENT MANAGEMENT

Incidents must be reported to IT directly through the "Top Desk" system. If that system is not available then the Service Desk can be contacted directly. In either case the information below should be given:

- Unique Identifier for the incident (assigned by the Top Desk system)
- Date and time of reporting and of incident (if different)
- Description of the incident
- Users, equipment, systems and information affected
- Suspected causes
- Any work around or other action taken to mitigate the impact

Other information is added after the incident has been investigated:

- Risk Assessment of the root cause of the incident
- All actions taken in response to the incident
- All escalations of the incident (who and when)
- Resolution of the issue
- Any outstanding actions to be completed (if applicable)
- Link to formal investigation, if required

APPENDIX 7 KEY PERFORMANCE INDICATORS

The purpose of these KPIs is to provide evidence as to the successful implementation of the policy. They are either absolute values (e.g. number of incidences of a particular nature) or relative values (increase/decrease in the number of incidences of a particular nature).

KPI Group	KPI	Description	Target
Acceptable Use	Inappropriate PID usage	Number of incidents where PID is used/shared inappropriately or in an unsecure way.	0 incidents
	Local drive storage	Number of incidents where data is stored on local drive instead of/as well as network drive.	0 incidents
	Website access	Access of inappropriate websites. Note than not all blocked websites are necessarily inappropriate so the number will be less than the total blocked.	Year-on-year reduction in number
Access	Password complexity	Number of passwords that are not at the required level of complexity.	Year-on-year reduction in number
	Generic accounts	Number of generic network domain accounts	No more than one
	Supplier accounts	Number of suppliers accounts without time-limited access	0 accounts
New Systems/ Infrastructure	New systems without CIO and BCRG approval	Number of new systems procured or deployed without following the process in this policy	0 systems
	New systems without IAO or IAA	Number of new systems introduced without identifying both the IAO and the IAA	0 systems

KPI Group	KPI	Description	Target
	New systems with PID/PIA/Board/SLSP/Clinical Safety Report	Number of new systems introduced without a PID, Project Board, SLSP, Clinical Safety Report and/or PIA for the deployment and use of it.	0 systems
Change Management	Changes without approval	Number of changes made to systems/infrastructure without approval by the relevant group	0 changes
	Legacy archive and exit	Number of new systems introduced without exiting from an existing system	0 systems
	Disposal	Number of devices/hardware disposed of without certified destruction of data held on it	0 devices
Cyber Security	Staff exit	Number of accounts not disabled within one week of IT being notified of a staff member leaving the job	0 accounts
	User-caused incidents	Number of incidents (e.g. virus, locally stored data, etc) caused by user behaviour in breach of policy. Note: May be initial increase due to encouragement to report	Year-on-year reduction in number once introduced
	EUD patch rollout	Time to rollout **critical** patches to EUD from notification by CareCert/supplier	1 day
	Server/network patch rollout	Time to rollout **critical** patches to infrastructure components from notification by CareCert/supplier	5 days
	EUD Admin account usage	Number of users with local admin rights	0

KPI Group	KPI	Description	Target
	Server admin account usage	Frequency of change of admin password across infrastructure	6 months
	Independent audit	Frequency of an independent audit (e.g. from NHS Digital) including penetration tests.	Annually
	Results of audit	Number of critical/high risk issues identified	Year-on-year decrease in number
	IAA	IAA identified and trained for all systems in use across Trust. Network of IAAs established with professional accountability to CIO.	Network established and 3-monthly meeting
GDPR/FOIA	Roles	Number of statutory/recommended roles not filled	0
	Staff training	Percentage of relevant/identified staff trained in GDPR, FOIA and IG matters	>95%
	Subject Access Requests	Number/percentage of requests not completed within statutory/recommended time limits	<5%
	FOIA Requests	Number/percentage of requests not completed within statutory/recommended time limits	<5%
	Breaches	Number of level 2 breaches of confidentiality	0
BYOD	Incidents	Number of incidents related to BYOD devices	Year-on-year reduction in number

KPI Group	KPI	Description	Target
DR and BC	Reports into disaster	Time taken to produce a report on a disaster after the end	1 month
	RPO/RTO	Number of systems without RPO and RTO defined	0

APPENDIX 8 NEW USER REGISTRATION FORM (EXAMPLE)

User Details			
Name:		Phone no:	
Organisation:		Department:	
Manager:		Main site:	
Group drives needed:			
NHSMail needed:	☐	Phone needed:	☐
Device needed:	Desktop/Laptop/Tablet/Other		
Type of user:	Employee/Contractor/Volunteer/Student/Other		

User Declaration			
I confirm that I have read the Digital Policy and will comply with the standards within it. I will safeguard the information that I have access to in line with the policy and legislation and will report any potential breaches of the policy.			
• I will not share my password with anyone nor let anyone log in to my account. • I will only access information relevant to the direct carrying out of my job. • I will safeguard the equipment given to me and return it when I no longer need it. • I accept that all equipment and information available to me remains the property of, and under control of, London North West University Healthcare NHS Trust.			
I will contact the Administrator for other systems that I require access to			
Signature:		Date:	

ICT Department to Complete			
User name:			
NHSMail address:			
Actioned by:		Date:	

APPENDIX 9 SYSTEM INFORMATION SHEET

To be completed by the Information Asset Owner & Administrator for each of their systems:

Systems details					
System name:			Supplier:		
Version in use:			Latest version:		
IA Owner:			Deputy:		
IA Administrator:			Deputy:		
Support email:			Support no.:		
Support times:			Hosting:		On premise/supplier
Architecture:	Browser/Thick/Thin		URLs:		
RPO:		RTO:		PIA ref:	
Depts. Using:					
Policy:					
Minimum length:			Maximum length:		
History length:	..... months		Complexity:		Enabled/Disabled
Logins attempts:	..... before lock		Expiry:		..... months
Signed (IAO):				Date:	
Signed (IAA):				Date:	

APPENDIX 10 SYSTEM LEVEL SECURITY POLICY

For each system (Information Asset), a System Level Security Policy (SLSP) must be written. The SLSP must contain a considered and specific view of the range of security policy and management issues relevant to the system and that may encompass a range of technical, operational and procedural security topics.

This must contain the following information:

- Names of the IAO and IAA
- Overview of the system architecture: where hosted, how accessed, etc.
  - Any remote access capability.
- Security features of the system:
  - Physical security of the servers
  - Authentication features
  - Network security (firewalls, etc)
  - Server security (port control, etc)
  - Password rules
  - Generic accounts
  - Admin accounts
- Roles and responsibilities of the IAO, IAA, super users, IT, suppliers and any other key roles in the management or security of the system.
- Confirmation that there are documented procedures for user access, roles/workgroup and audit.
- Training and awareness in the systems management
- How incidents will be managed (reporting, investigation, etc as earlier in this policy)
- Data flow maps for data in transit and at rest
- Disaster recovery plan
- Exit/archive plans
- Compliance: audit and monitoring of the security features of the system
- A risk assessment identifying possible risks to the information held on the system, and impact on Trust business operations.
- Segregation of access control roles that ensure that no single member of staff is able to authorise all access.

This report is needed for any new systems and needs to be reviewed for any changes to systems.

APPENDIX 11 CLINICAL SAFETY REPORT

Each system must have a Clinical Safety Report that sets out the impact that the system could have on clinical safety and shows the testing that has gone on to ensure little or no negative impact. The Clinical Safety Report will:

- Describe the system
- Set out the scope of the report
- Detail who is involved in clinical safety from both Trust and supplier side. This is the Clinical Safety Officer.
- Describe the activities that have taken place to construct the report (testing, workshops, etc)
- Summarise the issues that have been assessed as relevant to clinical safety, classified into High/Medium/Low/Very Low categories.
- Detail any "showstoppers" that would prevent a "Go Live" (this may be for a new system or for an upgrade to an existing system).

The Clinical Safety Officer must:

- Be a suitably qualified and experienced clinician.
- Hold a current registration with an appropriate professional body relevant to their training and experience.
- Be knowledgeable in risk management and its application to clinical domains.
- Make sure that the processes defined by the clinical risk management process are followed.

The clinical safety approach will leverage industry best practice, based on NHS Digital guidance and requirements and lessons learned from other NHS change programmes. The core elements of this approach include:

- **Mandatory Requirements**: Clinical Risk Management Processes as per ISB129 and ISB160 requirements for Health IT systems;
- **Roles and Responsibilities**: Trust and Supplier responsibilities to ensure that the appropriate clinical safety measures are established, including the resource to deliver.
- **Governance Arrangements**: Ensuring the appropriate structures are in place to manage the processes. Apart from the Project Board for the project, a Clinical Assurance Group may be appropriate. The Trust also has a Clinical Quality & Risk Committee and Patient Safety Committee – it may be appropriate for the Clinical Safety Report to be presented there.
- **Risk Management & Assurance**: Including the processes and tools are in place to identify, mitigate and monitor risks to enable the authorities to be assured of clinical safety. A Clinical Safety Log may be required to support this.
- **Clinical Safety Plan**: Detailed plan including key deliverables and dependencies.

NHS Digital has more detailed information, guidance and templates which should be consulted before carrying out a clinical safety assessment. This report is needed for any new systems and needs to be reviewed for any changes to systems.

A template for a Clinical Safety Report is available.

APPENDIX 12 PRIVACY IMPACT ASSESSMENT

Each system must have a Privacy Impact Assessment (PIA) which sets outs the impact that the system has on patient confidentiality. The Trust's template for PIAs should be used. The PIA will contain:

- Summary of the project and system under consideration
- Description of the information being collected, how it stored and how it is to be used.
- Details on the information flows within and outside of the system
- The type of information being used and the media involved
- A summary of where and with who the PIA has been discussed
- A risk assessment of the information, including any mitigating steps that can be taken
- Details on any sharing of the information with third parties

This report is needed for any new systems and needs to be reviewed for any changes to systems.

APPENDIX 13 EQUALITY IMPACT ASSESSMENT SCREENING TOOL

Directorate / Department		ICT and Systems	
Policy or Operating Procedure or Guidelines Title / Service		Digital Policy	
Name and role of Assessor		Natasha Beach, Associate Director of ICT	
Date of Assessment		4th May 2018	
		Yes/No	Comments
1	Does the policy/Guideline affect one group less or more favourably than another on the basis of:		
	Race, Ethnic Origins (including gypsies and travellers) and Nationality	No	
	Gender (including gender reassignment)	No	
	Age	No	
	Religion, Belief or Culture	No	
	Disability – mental, physical and learning disability	No	
	Sexual orientation including lesbian, gay and bisexual people	No	
	Married/or in civil partnership	No	
	Pregnant	No	
2	Is there any evidence that some groups are affected differently?	No	
3	Is there a need for external or user consultation?	No	
4	If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?	No	
5	Is the impact of the policy/Guideline likely to be negative?	No	
6	If so, can the impact be justifiable?	NA	
7	What alternatives might enable achievement of the policy/ guidelines without the impact?	NA	
8	Can we reduce the impact by taking different actions?	NA	
Recommendation Full Equality Impact Assessment required: NO			
Assessor's Name: N Beach Date: 4th May 2018			