Kent Community Health
NHS Foundation Trust

Cyber, Network and Information Systems Policy

Document Reference No.	KIG026
Status	FINAL
Version Number	1.2
Replacing/Superseded policy or documents	1.0
Number of Pages	53
Target audience/applicable to	All individuals working for, and on behalf of the organisation including temporary workers, locums and volunteers
Author	Cyber Security Specialist
Acknowledgements	
Contact Point for Queries	Cyber Security Specialist
Date Ratified	March 2021 (Previously May 2018)
Date of Implementation/distribution	March 2021
Circulation	Intranet, Policy Distribution
Review date	May 2024
Copyright	Kent Community Health NHS Foundation Trust

EXECUTIVE SUMMARY

This Cyber, Network and Information Security policy (CNIS) is a key component of Kent Community Health NHS Foundation Trust's Information security management framework.

Data stored in computer systems represents an increasingly valuable asset to the Trust as its systems continue to grow and increased reliance is placed upon them.

Additionally, organisations have a legal responsibility under the current data protection law to ensure the secure storage, use, transmission and when no longer required, the secure destruction of these data assets.

Breaches of data protection legislation may result in distress to patients, reputational damage and punitive stating fines may be levied for reckless breach of data protection legislation.

The Trust seeks to protect its computer systems from misuse and minimise the impact of service disruption by developing a Cyber, Network and Information Systems Policy and procedures.

Key points addressed by the Cyber, Networking and Information Security Policy are:

a) To document the processes and controls in place to protect the Trusts IT infrastructure, Network, and assets including its data and that of its patients.
b) To understand the counter measures deployed to meet the threats.
c) To give all staff an understanding of their role in keeping the organisation safe from cyber threats.
d) To ensure the Trust is compliant with all relevant regulations (For example GDPR, Data Protection Act 2018, 10 Data Guardian Security Standards and Network Information Systems (NIS) Regulations 2018

Scope and purpose of Policy

This Cyber, Network, and Information Systems Policy (CNIS) is intended to support the protection, control and management of ALL the Trust's electronic information assets (PC's, Hard Disks, external media, USB devices, servers etc.) and supporting infrastructure, including the network.

The Policy covers all information within the Trust and can include data and information which is stored on:

a) Stored in databases
b) Stored on Computers
c) Transmitted across internal and external networks
d) Printed or hand written on paper or white boards or similar.
e) Stored on removable media such as CDs, DVDs, Memory sticks or other USB removable media, hard drives, tapes or similar media.
f) Presented on slides, overhead projectors, using visual or audio media.
g) Spoken during telephone calls and meetings or conveyed by any other method. This includes applications like Teams or similar video conferencing programs.

The Trusts Cyber, Network and Information Security policy aims to ensure:

a) The Trust is kept as secure as possible from cyber risks and threats.
b) Confidentiality, integrity and availability of data and systems is maintained
c) All individuals working for, and on behalf of the organisation are aware of the evolving threats and their responsibilities, roles and accountability in mitigating them.
d) Procedures to detect, resolve, and report cyber incidents are in place.
e) The Trust is able to continue its activities in the event of a cyber security breach.
f) Accountability and governance responsibility is maintained by the Senior Information Risk Owner (SIRO), Caldicott Guardian (CG) and the Data Protection Officer (DPO)
g) To follow and apply NHS Digital best practice guidance, and the National Data Guardians 10 Data Security Standards which form the basis for the Data Security and Protection Toolkit.
h) To Apply the National Cyber Security Centres (NCSC) "10 Steps to Cyber Security"
i) To meet compliance with the EU General Data Protection Regulation, Data Protection Act 2018 and Networks and Information Systems (NIS) Directives as fines may be levied for reckless breach of data protection legislation, or failing to meet "Best Practice" minimum standards.
j) To apply the standards required in order for the Trust to achieve the Cyber Essentials Plus Certification.
k) Protection of the organisations reputation as an outstanding trust.

For further information on confidentiality legislation and the National Data Guardians 10 data standards see the Data Security and Protection Policy.

For more information on the National Cyber Security Centre see their website at https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

For more information on the Network Information Security Directive (NIS) see https://www.ncsc.gov.uk/guidance/introduction-nis-directive

It is important to note that this Policy is only one of a group of policies, and SOPs that make up the Trust's overall security plans. All individuals working for, and on behalf of the organisation must be aware of their obligations under the other policies. This includes 3rd Party providers who are granted access to the network for any reason, and temporary staff employed either directly by the Trust or through an external agency. Such individuals will be referred to as "staff" or "users" throughout this Policy.

Any member of staff in breach of information security contained within this policy or other policies or SOPs supporting it, may be subject to the organisations disciplinary procedure and be dismissed from employment if deemed appropriate.

Risks addressed

Cyber-attacks are an increasing and evolving threat for all NHS (and other) organisations. Whilst the Trust continues to refresh and deploy a number of technical counter measures, these in themselves will only go so far in protecting the organisation from attack. The biggest risk to the organisation is the behaviour of the individuals working for, and on behalf of the organisation, who may inadvertently (or deliberately) infect the organisation with malware deployed by increasingly sophisticated means. This policy provides a framework for all individuals to understand the totality of the Trust's defences and their

own role in mitigating the threat from cyber-attacks. The ways in which we address these risks are:

- **Risk Management**
- **Secure configuration**
- **Network security**
- **Managing user privileges**
- **User education and awareness**
- **Incident management**
- **Malware prevention**
- **Monitoring**
- **Removable media controls**
- **Home and mobile working**
- **Physical Security**

This policy applies to all Networks, and IT Systems within the Trust used for:

a) The storage, sharing and transmission of non-clinical data and images.
b) The storage, sharing and transmission of clinical data and images.
c) Printing or scanning non-clinical or clinical data and images.
d) The provision of Internet and email systems for receiving, sending/sharing and storing non-clinical and clinical data and images.

NOTE: This collection will be referred to as the “Trust network” throughout the document, and includes Printers, Photocopiers, Franking machines, Point-of-sales (POS) devices, Desktop PC’s, Laptops, Servers, Routers, Switches, Wireless Access Points (WAPs), Mobile and medical devices.

It is important that all staff be made aware, through documentation, training and awareness that they must meet Information Governance requirements and that is made clear to them that breaching these requirements either deliberately or negligently is a disciplinary offence.

The framework’s ultimate goal is to help the Trust and its staff to be consistent in the way they handle personal confidential and corporate information and to avoid duplication of effort, which will lead to improvements in information handling activities, patient confidence in care provision and employee training and development.

Governance Arrangements

Governance Group responsible for developing document	Information Governance Assurance Group
Circulation group	All individuals working for, and on behalf of the organisation through Flo, public website.
Authorised/Ratified by Governance Group/Board Committee	Information Governance Assurance Group and Corporate Assurance Risk Management Committee.
Authorised/Ratified On	Renewed March 2021
Review Date	March 2024
Review criteria	This document will be reviewed prior to review date if a legislative change or other event dictates.

Key References

These are key documents that the policy relies on for best practice or national guidance or a legislative requirement. It is a list of those items that have been relied on for best practice and influence the requirements of the policy.

Data Security Protection Toolkit
Police and Criminal Evidence (PACE) and Terrorism Act
Information Security Management Code of Practice (2007)
Freedom of Information Act
General Data Protection Regulation (GDPR) 2018
Computer Misuse Act (1990)
Data Protection Act (DPA 2018)
BS ISO / IEC 27001: 2013 Information Security Management
Records Management Code Of Practice for Health and Social Care
The Protection and Use of Patient Information
Manual for Caldicott Guardians 2017
Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation
Good Practice Guides - NHS Digital
10 Steps to Cyber Security - NCSC
The EU Directive on the security of network and information systems (NIS) 2018
Public Records Act 1967
Ensuring Security and Confidentiality in NHS Organisations. (E5498) January 1999
Human Rights Act (1998)
Health Service Guidance (HSG (96) 18) – The Protection and Use of Patient Information
Health and Social Care Cloud Security – NHS Digital
Health and Social Care Data Risk Model – NHS Digital
National Data Guardians 10 Data Security Standards
Cyber Essentials Plus Certification Scheme

Related Policies/Procedures

These are key policy documents that the policy relies on for further guidance and best practice.

Title	Reference
Data Security and Protection Policy	KIG025
Home, remote and mobile working SOP	KIG034
Flo App SOP	KIG035
IT Evidence Seizure SOP	KIG032
Use of Email SOP	KIG031
Instant Messaging IM SOP	KIG033
Third Party Open Access and Remote Connection SOP	NA (IT Internal Policy)
Video Conferencing and Consultations SOP	KIG030
Whistleblowing policy and procedure	HR010
Registration Authority Policy	RAM001

Document Tracking Sheet

Version	Status	Date	Issued to/Approved by	Comments/Summary of Changes
0.1	DRAFT	01/02/2018		Merged the network sec policy (KIG010) and the information sec policy (KIG009)
0.2	DRAFT	15/03/2018		Incorporated the IT disposal policy (KIG.020), forensic readiness policy (KIG019) and cyber security policy (KIG022).
0.3	DRAFT	25/04/2018		Final additions and amendments in line with Cyber Essentials Plus requirements, circulated for 2-week consultation.
0.3	DRAFT	09/05/2018	IGAG	Approved subject to feedback from consultation
0.3	FINAL	May 2018	CARM	For virtual approval. Formatting and numbering tidied, key reference and related policies and procedures updated
1.0	Final	May 2018	Compliance Officer	Formatting and numbering tidied, key reference and related policies and procedures updated, version number updated and published
1.1	Final	August 2018	IT Cyber Security Specialist	Points L, M, N, O added to section 5.17 Section 12.8 added Numbering tidied

1.2	FINAL	0	IGAG (Virtual)	Updates required due to change in work practices after COVID-19 and general additions required due to changes to compliance requirements. Incorporated “Mobile communication and teleworking policy”.

CONTENTS

1.0 INTRODUCTION

1.1 In recent years the instances of organisations being subject to cyberattack has significantly increased to the point where it is essential that all organisations take the necessary steps to protect themselves. The ways in which organisations protect themselves is referred to as cyber security and is composed of both technical and human countermeasures.

1.2 The Trust has legal obligations to maintain the confidentiality, integrity and availability of the Trusts IT systems, network and data.

1.3 This policy is designed to inform Trust employees, contractors and other authorised users of their obligatory requirements for protecting the technology, network and information assets of the Trust. It also describes those assets that must be protected and identifies some of the known threats to those assets and the countermeasures deployed by the Trust to mitigate them.

1.4 Equality, Diversity and Inclusion

1.4.1 Communication and the provision of information are essential tools of good quality care. To ensure full involvement and understanding of the patient and their family in the options and decision making process about their care and treatment, all forms of communication (e.g. sign language, visual aids, interpreting and translation, or other means) should be considered and made available if required. These principles should be enshrined in all formal documents.

1.4.2 Kent Community Health NHS Foundation Trust is committed to ensuring that patients whose first language is not English receive the information they need and are able to communicate appropriately with healthcare staff. It is not recommended to use relatives to interpret for family members who do not speak English. There is an interpreter service available and staff should be aware of how to access this service.

1.4.3 The privacy and dignity rights of patients must be observed whilst enforcing any care standards e.g. providing same sex carers for those who request it. (Refer to Privacy and Dignity Policy).

1.4.4 Kent Community Health NHS Foundation Trust is committed to ensuring that information is provided in accessible formats and communication support is met for people (patients, carers, parents/guardians) with a disability, impairment or sensory loss. The Accessible Information Standard (AIS) is a legal requirement of the Equality Act 2010 which applies to all organisations included within the Health and Social Care Act.
https://www.england.nhs.uk/ourwork/patients/accessibleinfo/. Guidance on professional support services for the Trust is available in the Accessible Information Policy.

1.4.5 Staff must be aware of personal responsibilities under Equality legislation, given that there is a corporate and individual responsibility to comply with Equality legislation. This also applies to contractors when engaged by the Trust, for NHS business.

1.5 Equality Analysis

1.5.1 Kent Community Health NHS Foundation Trust is committed to promoting and championing a culture of diversity, fairness and equality for all our staff, patients, service users and their families, as well as members of the public.

1.5.2 Understanding of how policy decisions, behaviour and services can impact on people with 'protected characteristics' under the Equality Act 2010 is key to ensuring quality and productive environments for patient care and also our workforce.

1.5.3 Protected Characteristics under the Equality Act 2010 are:

- Race
- Disability
- Sex
- Religion or belief
- Sexual orientation (being lesbian, gay or bisexual)
- Age
- Gender Re-assignment
- Pregnancy and maternity
- Marriage and civil partnership

1.5.4 An equality analysis should be completed whilst a policy is being drafted and/or reviewed in order to assess the impact on people with protected characteristics. This includes whether additional guidance is needed for particular patient or staff groups or whether reasonable adjustments are required to avoid negative impact on disabled patients, carers or staff.

1.5.5 The Equality Analysis for this policy is available upon request by contacting the Engagement Team via kchft.equality@nhs.net.

2.0 ROLES AND RESPONSIBILITIES

2.1 The Trusts Objective

2.1.1 To ensure that anyone working for and on behalf of the Trust are aware of IT and Cyber security risks and their responsibilities to minimise the risks.

2.2 Individual Responsibility

2.2.1 All staff are responsible for familiarising themselves with all policies and procedures concerning Information Security as they relate to their working activities and as defined in every contract of employment.

2.3 Senior Management

2.3.1 The Chief Executive is the senior accountable officer for the enforcement of this policy. The Chief Executive has overall responsibility for all aspects of the management of this policy and the Cyber/Information Security of the Trust. Senior Management responsibilities are as stated below;

a) To ensure that the National Data Guardian's 10 Data Security Standards are met.

b) To ensure all current and future staff are instructed in their security responsibilities
c) To ensure all their staff using computer systems/media are trained in their use
d) To ensure no unauthorised staff are allowed to access any of the Trust's computer systems as such access could compromise data integrity
e) To implement procedures to minimise The Trust' exposure to fraud/theft/disruption of its systems, these may include segregation of duties/dual control/staff rotation in critical susceptible areas
f) To ensure current documentation is always maintained for all critical job functions to ensure continuity in the event of individual unavailability
g) To ensure staff are aware of the Trust' Standing Orders on potential personal conflicts of interest
h) To ensure all staff sign confidentiality (non-disclosure) undertakings as part of their contract of employment
i) To ensure all related mandatory training is completed as required

2.4 Head of IT

2.4.1 The responsibilities of the Head of IT are:

a) To ensure that the National Data Guardian's 10 Data Security Standards are met.
b) To ensure IM/IT equipment is sited or protected to reduce risks from environmental threats and hazards, and unauthorised access
c) To ensure that data held on systems is backed up on a regular basis (daily, weekly, monthly) depending upon the usage and critical nature of the system. Backups can be of the whole system or only of changes since last backup ('incremental')
d) To ensure that all backup copies are held either off-site, or in a fire-resistant cabinet suitable for the materials in use
e) To ensure IM/IT equipment purchases are added to the organisation's inventory, is security labelled, with appropriate licensed software loaded, and the equipment suitably configured for use
f) To authorise computer hardware disposal via the Director of Finance, ensure it is deleted from the Trust's inventory, and ensure data storage devices are purged of confidential data before disposal or securely destroyed
g) To ensure that all disposals of computer equipment meet current National and EU Regulations
h) To ensure that a list of current authorised users is maintained at all times
i) To ensure that a current list of IT systems is maintained at all times
j) To ensure that correct vetting procedure is followed while selecting the Disposal Company.
k) To ensure that a Data Privacy Impact Assessment (DPIA) is carried out prior to the start of any project that involves an IT system and personal confidential information.
l) To ensure that all new processes, software/hardware, involving personal confidential information complies with Data Protection and Confidentiality, and Information Governance audits

2.5 Senior Information Risk Owner

2.5.1 The Senior Information Risk Owner (SIRO) will be an Executive or Senior Manager on the board

a) To ensure that the National Data Guardian's 10 Data Security Standards are met.
b) Ensuring appropriate Data Protection Act (the Act) notification is maintained for the Trust' systems and information
c) To oversee the development of Information Risk outlined in the Data Security and Protection Policy
d) Review of the annual information risk assessment to support and inform the Statement of Internal Control
e) To take ownership of risk assessment process for information risk, including to review and agree action in respect of identified information risks
f) To ensure that the organisation's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff
g) To provide a focal point for the resolution and/or discussion of cyber or information risk issues
h) To ensure the board is adequately briefed on information and Cyber risk issues.

2.6 Data Protection Officer (DPO)

2.6.1 The responsibilities of the DPO are:

a) To ensure that the National Data Guardian's 10 Data Security Standards are met.
b) Ensuring that the Trust complies with all aspects of Information Governance and provide reports to the Board via the Information Governance Assurance Group
c) To draft and/or maintain the Trust' Data Security and Protection Policy and ensure that it meets current legislation and best practice.
d) To promote Information Governance awareness throughout the Trust by organising training and providing written procedures that are widely disseminated and available to all staff
e) To co-ordinate the work of other staff with Information Governance compliance responsibilities
f) To ensure patients are provided with information on their rights under data protection legislation
g) To monitor Information Governance compliance and the effectiveness of procedures through the use of compliance checks/audits and ensure appropriate action is taken where non-compliance is identified
h) To assist with investigations into complaints about breaches of Information Governance
i) Advising the Information Governance Assurance Group on breaches of compliance, and recommend actions for mitigating the risks
j) Dealing with enquiries about Information Governance compliance
k) Liaising with external organisations on Information Governance matters

2.7 Committees

2.7.1 Information Governance Assurance Group (IGAG)

2.7.2 The responsibility of the Information Governance Assurance Group is to operate as an oversight body for the co-ordination and communication of the policy throughout

the organisation. Also to seek assurance on current risks from the accountable service leads and to escalate if required.

2.7.3 Corporate Assurance and Risk Management (CARM)

2.7.4 The operational management of risk is central to the Executive Team's role which performance manages the Board Assurance Framework (BAF) and Corporate Risk Register (CRR) on a monthly basis. To support this, each Director, with their operational teams, reviews and manages their Directorate Risk Register on a monthly basis which culminates in the production of the Corporate Risk Register and BAF for presentation to the Executive Team. The BAF lists agreed high rated risks and the CRR lists risks rated above a specific threshold. The Executive Team considers whether risks listed on the Corporate Risk Register are significant enough to be escalated on to the BAF. In addition to the escalation of high rated risks described above, the Corporate Assurance and Risk Management (CARM) Group reviews trends in lower rated risks, and where it is considered that these are indicative of a more serious organisational risk than implied by the individual risk scores, this is reported to the Executive Team to be considered for escalation on to the BAF. High risks identified through this process are documented on the BAF, and the mitigation of these risks is monitored by the Board.

2.8 IT Systems Managers (Infrastructure)

2.8.1 The responsibilities of IT Systems Managers are:

a) To understand and meet their own responsibilities, and ensure staff are aware of their obligations under the National Data Guardian's 10 Data Security Standards
b) To ensure job descriptions for their posts include specific reference to the security role and responsibility of the post
c) System managers will be responsible for conducting confidentiality audits in liaison with the Cyber Security Specialist. These should include, but are not limited to, the monitoring and auditing of:
    i. failed attempts to access confidential information
    ii. repeated attempts to access confidential information
    iii. successful access of confidential information by unauthorized persons
    iv. evidence of shared login sessions/passwords
    v. disciplinary actions taken
d) System managers will be responsible to the Cyber Security Specialist for continued system security
e) To ensure that all new processes, software/hardware, involving person confidential information complies with Data Protection and Confidentiality requirements.
f) To ensure that points 3.0 through 16.0 of this policy are implemented in relation to their area of responsibility.

2.9 Information Asset Owners (IAOs – Also known as Application Managers)

2.9.1 For information risk, IAOs are directly accountable to the Cyber Security Specialist and will provide assurance that information risk is being managed effectively for their assigned information assets (systems). IAOs may be assisted in their roles by staff acting as Information Asset Administrators - IAAs (or persons with equivalent responsibilities) who have day to day responsibility for management of information risks affecting one or more assets.

2.9.2 The responsibilities of the Information Asset Owners are:

a) It is particularly important that each IAO (or equivalent) should be aware of what information is held on each information asset (system) and the nature of and justification for information flows to and from the assets for which they are responsible.
b) The role of the IAO is to understand what information is held, what is added and what is removed, how information is moved, who has access and why. As a result they should be able to understand and address risks to the information and to ensure that information is fully used within the law for the public good.
c) The IAO is responsible for ensuring that the information assets they own have documented approved access controls in place for each key information asset under their control, and that these controls are regularly reviewed and reports documented to show access is only possible to authorised users.
d) It is important that “ownership” of Information Assets is linked to a post, rather than a named individual, to ensure that responsibilities for the asset are passed on, should the individual leave the organisation or change jobs within it.
e) To ensure the relevant system managers are advised immediately about staff changes affecting computer access (e.g., job function changes or leaving department or organisation) so that accounts may be withdrawn or deleted Ensure the asset is maintained to ensure it meets the standards laid out in this policy.
f) As a minimum conduct annual user account reviews on systems under their responsibility.

2.9.3 See also Section 2.8 Responsibilities of IT Systems Managers for more guidance

2.10 Managers

2.10.1 The responsibilities of Managers are:

a) To ensure all current and future staff are instructed in their security and Information Governance responsibilities
b) To ensure all their staff using computer systems/media are trained in their use
c) To ensure no unauthorised staff are allowed to access any of the Trust’ computer systems, as such access could compromise data integrity
d) To determine which individuals are to be given authority to access specific computer systems. The level of access to specific systems should be on a job function need, independent of status
e) To implement procedures to minimise exposure to fraud/theft/disruption of its systems, such as segregation of duties/dual control/staff rotation in critical susceptible areas

f) To ensure current documentation is always maintained for all critical job functions to ensure continuity in the event of individual unavailability
g) To ensure staff are aware of the Trust' Standing Orders on potential personal conflicts of interest
h) To ensure the starters and leavers procedure is followed in a timely manner.
i) To ensure any and all IT equipment allocated to their direct reports is logged and tracked to ensure the IT items' location is auditable for its lifetime, and is returned as part of the leaver's process without exception.
j) To ensure staff are aware of their security incident reporting procedures (Datix)
k) To ensure that DPIAs are completed for all systems which store, or interact with, personally identifiable information (PII). Also that the IT section of the DPIA is completed where required for any new IT system.
l) To ensure that the correct process is followed for implementing any new IT system (including local software installs, KCHFT internally hosted applications, and any cloud or web-based system)

2.11 Staff

2.11.1 Staff responsibilities are:

a) To understand their obligations under the National Data Guardian's 10 Data Security Standards.
b) Each employed, contracted and voluntary member of staff is personally responsible for ensuring that no breaches of information security result from their actions
c) Each staff member (as above) must comply with the organisation's security policies and procedures. Breaches will be subject to a formal investigation, and if found to be deliberate, may lead to disciplinary action which may lead to legal action
d) Each staff member is personally responsible for the accuracy and currency of the data they record on systems
e) Each staff member should declare any potential conflicts of interest as required by the organisation's Standing Orders
f) To ensure confidential information is stored on the network where backups are taken daily (i.e. mobile devices are not to be used as storage devices)
g) Where personally identifiable data is held on mobile devices and removable media such as Phones, USB sticks, diskette, DVDs/CDs, to be responsible for ensuring that they are stored on **only** encrypted media provided or authorised by the organisation for use and have relevant password protection
h) To read and understand the Cyber Network and Information Systems Policy
i) To read and understand the Data Security and Protection Policy
j) The security of the physical environment is maintained as laid out in KCHFT Policies.
k) Any KCHFT equipment or records must only be transported in a secure bag or rucksack. If transported in a car, the equipment or records must be kept out of sight, in the boot, and never left in the car overnight. If the equipment or records are to be held at a staff members' home, it is their responsibility to ensure the safety of the equipment and information held, and that it is not accessible to anyone not authorised to see it.
l) To ensure all physical IT equipment is returned at the end of employment without exception.

2.12 Specialist Role

2.12.1 The responsibilities of the Cyber Security Specialist are:

a) To ensure that the National Data Guardian's 10 Data Security Standards are met.
b) Responsible for implementing, monitoring, documenting and communicating information security within the Trust, in compliance with UK legislation and national policy and guidance
c) Responsible for monitoring and reporting the state of Cyber security within the Trust
d) To ensure the Cyber, Network and Information Systems Policy is implemented and monitor compliance throughout the Trust
e) To ensure relevant staff are aware of their security responsibilities and that security awareness training is provided for all users
f) To monitor for actual or potential information or Cyber security breaches within the Trust
g) Ensuring procedures to detect and resolve security breaches are in place
h) Monitoring and reporting on the state of Cyber security within the Trust
i) Working with the Risk Management team, monitoring for actual or potential Information security breaches and ensure all identified risks and breaches are logged and handled appropriately
j) Developing and enforcing detailed procedures to maintain security
k) Ensuring compliance with relevant legislation
l) Ensuring the Trust personnel are aware of their responsibilities and accountability for Information Security
m) Performing internal audits of all information systems/assets and/or arranging for external auditors

2.13 Caldicott Guardian

2.13.1 The responsibilities of the Caldicott Guardian are:

a) To be responsible for strategy and governance and to champion confidentiality issues at board/management team level and act's as the "conscience" of the Trust and the enabler of appropriate and secure information sharing of patient information
b) Responsible, on behalf of the Chief Executive, for agreeing, monitoring, and reviewing internal protocols governing access to patient confidential information by staff within the Trust, in compliance with UK legislation and national policy and guidance
c) Responsible for agreeing, monitoring, and reviewing protocols governing the use of patient confidential information across organisations, e.g. with other NHS and local authority services, and other partner organisations contributing to the local provision of care
d) To ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff

2.14 IT Teams

2.14.1 The IT Teams are organised as follows;

a) System
b) Network

c) Telecom
d) Cyber Security
e) Infrastructure
f) Service Desk
g) Mobile Management
h) CIS
i) RIO
j) Information Asset Owners
k) Projects/Applications

2.14.2 Each IT Team is responsible for their relevant processes and procedures laid out in this document, that all Team members are aware of them, adhere to them and that they follow best practice, being regularly reviewed internally by each team. In certain cases these processes will be reviewed by the Cyber Security Specialist and Senior IT Manager if required.

2.14.3 Each Team is also responsible for the patching of the equipment they are directly responsible for to ensure both OS versions and software are up to date, with vulnerabilities patched within a reasonable timeframe.

2.14.4 Each IT Team is responsible for responding to and remediating CareCERTs which fall under their responsibility.

2.14.5 Each IT Team will follow the Trusts Request For Change (RFC) procedure to ensure all significant changes are approved by relevant IT Team members/Responsible Managers.

2.15 Other Authorised Users

a. Other NHS and authorised external users are personally responsible for ensuring that no breaches of computer security result from their actions
b. To comply with the organisation's security policies and procedures
c. To ensure any data stored regarding, or on behalf of the Trust is stored with appropriate controls in line with all legal requirements and the specifications laid out in the Trusts Data Protection Impact Assessment (DPIA) IT security assessment questions.

3.0 RISK MANAGEMENT

3.0.1 Risks are a necessary part of business and delivering any kind of service. To operate legally and successfully the Trust must identify risk and respond appropriately depending on whether it is a risk the Trust is willing to accept.

3.1 Risk Assessments

3.1.1 The Trust will identify, then either mitigate or accept the risks associated with the probability of a threat exploiting vulnerability in the Trust.

3.1.2 The Trust will carry out risk assessments in relation to IT systems and business processes covered in this policy based on the ISO 27001 framework, the trusts Risk Register (Datix), NHS Digitals Unified Cyber Risk Framework or the KCHFT DPIA document. These will be carried out by System owners or Managers (Including

Project Managers where applicable) and must include all aspects of the delivery of the System and Service.

3.1.3 The Trust has a DPIA process which contains an IT risk assessment section which can also be used to assess any IT risk and provide additional assurances where required around IT systems.

3.2 Data Protection Impact Assessments

3.2.1 The Trust is legally mandated to carry out a Data Protection Impact Assessment (DPIA) for all internal and external systems which handle the Trusts person identifiable data. These will be in line with NHS Digital and NIS framework. DPIAs will be reviewed once every 3 years, when there is a change in use, change in data type, or during renewal of contract. These will be carried out by System owners or Managers (Including Project Managers where applicable) and must include all aspects of the delivery of the System and Service. All DPIAs will need approval from both the IG Team and the Cyber Security Specialist, prior to being authorised on behalf of the organisation by the Data Protection Officer. See Flo for DPIA guidance and the Data Security and Protection Policy for further guidance.

3.3 Assessment of all Systems Relating to IT

3.3.1 All IT systems must be assessed using the IT section of the KCHFT DPIA before being put into use by the Trust. This includes Systems or applications which do not hold, store or relate to PII or Patient data.

3.3.2 The procurement of all new IT systems should go through the correct process via the IT Project Team.

3.3.3 Any system in use should be reviewed by the application owner at least every three years completing a new risk assessment.

3.4 External Alerting and Knowledge Sharing Partnerships

3.4.1 The Trust will enter into knowledge sharing partnerships to help understand emerging threats, and how they could affect the Trust. Where possible the Trust will join organisations which offer an “Early Alerting Framework”, which will be used in conjunction with CareCERT to increase likelihood of the Trust being aware of new vulnerabilities.

3.5 Risk Lifecycle

3.5.1 All systems will be subject to periodic security reviews by system managers. The depth of a review will be determined by the importance and size of the particular system.

3.5.2 Individual systems should be reviewed at least once every three years. Reviews will include:

a) identification of assets of the system;
b) evaluation of potential threats;
c) assessment of likelihood of threats occurring;
d) identification of practical cost effective counter measures;

e) implementation programme for counter measures;

3.5.3 Systems are liable to independent reviews by internal and external auditors. Each system review will include a formal report to the Trust Cyber Security Specialist.

3.6 Information Governance Assurance Group (IGAG)

3.6.1 IGAG will monitor IG risk and risk trends throughout the Trust gaining assurance from relevant departments, taking action or passing to CARM where required.

3.7 Corporate Assurance and Risk Management Group (CARM)

3.7.1 The operational management of risk is central to the Executive Team's role which performance manages the Board Assurance Framework and Corporate Risk Register on a monthly basis. To support this, each Director, with their operational teams, reviews and manages their Directorate Risk Register on a monthly basis which culminates in the production of the Corporate Risk Register and BAF for presentation to the Executive Team. The BAF lists agreed high rated risks and the CRR lists risks rated above a specific threshold. The Executive Team considers whether risks listed on the Corporate Risk Register are significant enough to be escalated on to the BAF. In addition to the escalation of high rated risks described above, the Corporate Assurance and Risk Management (CARM) Group reviews trends in lower rated risks, and where it is considered that these are indicative of a more serious organisational risk than implied by the individual risk scores, this is reported to the Executive Team to be considered for escalation on to the BAF.

4.0 SECURE CONFIGURATION

4.0.1 The Trust will establish and actively maintain the secure configuration of our systems, and make formal assessments of 3rd party systems providing services on our behalf. If systems are not effectively managed they can be more vulnerable to attack, and in some cases a breach may occur which could have been prevented. This also includes misconfiguration by authorised staff, and poor Change Control Procedures being in place.

4.1 Standardisation

4.1.1 Each IT Team will document the build design for each asset, and these documents must be followed for every asset provided by KCHFT.

4.1.2 Where possible a secure baseline build for hardware and software will be implemented. Baseline configurations must be continually monitored by responsible IT Team and all non-essential services, ports and functionality must be removed or disabled when their use is not necessary to eliminate unnecessary risk.

4.1.3 Old functionality and software no longer required by the Trust should be disabled or removed.

4.1.4 IT baselines should be managed and controlled with any deviations documented and approved by responsible IT Team Manager, and the IT RFC procedure..

4.1.5 Ensure that any default credentials on all equipment are changed to meet the Trusts password standard requirements. See section **6.2 Passwords**

4.1.6 All base images for all IT equipment must implement security hardening as recommended by a reputable third party organisation.

4.1.7 Ensure that the operating system on all new hardware and equipment is updated to the latest version, or latest secure version which is in use on existing equipment.

4.1.8 All IT equipment must be responsibly sourced from legitimate providers to ensure integrity of the equipment.

4.2 Supported and Licenced Software

4.2.1 The Trust will only use software which is still actively supported. In the case that support for a product is removed the Trust will take steps to source a replacement, stop use altogether or use other controls to reduce the risk. Any exceptions require SIRO authorisation, and be recorded in the KCHFT risk register.

4.2.2 All users should ensure that they only use licensed copies of commercial software. It is a criminal offence to make or use unauthorised copies of commercial software. Offenders are liable to disciplinary action and civil and criminal prosecution

4.2.3 The Trust will only permit approved software to be installed on its PCs, laptops, and mobile devices. Senior IT managers and/or the Cyber Security Specialist will approve all software, and the KCHFT IT service will install, or oversee the installation of all software. This will be controlled by security policies set on the local machines via Group Policy, access controls, and/or centralised management platforms.

4.2.4 Where non-approved software or systems are in use, these must be phased out as soon as practicable. This includes legacy systems, or historic controls.

4.2.5 Where the Trust recognises the need for specific specialised PC products, such products should be registered with KCHFT and be fully licensed.

4.2.6 The Trust will also have processes in place to allow the monitoring and reporting of all software used, so that out of date or unsupported software can be identified and the required action taken.

4.2.7 This applies to all operating systems and software used by the Trust not just desktops/laptops and servers, it also includes all Network equipment (Routers/switches/firewalls), mobile devices including smart phones, medical devices and Printers.

4.2.8 Using or copying computer software or other intellectual property in violation of licence or copyright agreements in strictly prohibited.

4.2.9 Where legacy systems cannot be removed, every exception to this policy must be recorded in the KCHFT Risk Register, and be approved by the SIRO with strong risk reducing, and mitigation controls in place.

4.3 Updating and Patching

4.3.1 The Trust will have procedures and controls in place to monitor the patch level of the IT Estate, and report on the level of compliance, including the use of automated tools.

4.3.2 Each IT Team is ultimately responsible for their respective systems, for ensuring that the systems in use are fit for purpose, they are aware of available updates or Security patches and that they are applied so an acceptable level is maintained.

4.3.3 Each IT Team will have a patching policy or SOP which details the patch management of the devices and hardware under their area of responsibility.

4.3.4 The Update and Patch level of IT systems and hardware should be centrally managed wherever possible to allow oversight and auditing/reporting.

4.3.5 In the event of a CareCERT where an emergency patch is required, immediate action should be taken to assess the relevance of the CareCERT to the Trust and if an emergency patch schedule is required. For more information on CareCERTs visit https://digital.nhs.uk/cyber-alerts

4.3.6 Where updates or patches cannot be applied as it would cause system damage, make an existing system unable to perform its function impacting on patient care, the risk must be assessed using appropriate frameworks (See section 3.0 Risk Management). The risk should then be presented to the appropriate groups (IGAG/CARM) where it will either be accepted or rejected, or passed to DPO or SIRO for further investigation.

4.4 Managing IT Systems

4.4.1 All IT Teams and system owners will have a recorded process in place for starters movers and leavers for user accounts to systems under their responsibility not managed by the IT Team, and all user accounts must be set up in accordance with these documents. The process should ensure that staff have only the permissions required to carry out their role, and that accounts are disabled immediately upon end of employment within the trust. 6 monthly user account audits should be carried out.

4.4.2 You must not implement any new IT system either on premise, or cloud based without first contacting the IT Project team. This includes systems where PII will not be used. All systems must be assessed by IT prior to use, and DPIA's must be completed where required.

4.5 Vulnerability Management

4.5.1 The Trust will implement a vulnerability management process where Penetration Tests and Vulnerability scans will provide information on potential issues, or existing vulnerabilities on the Trusts network. The Trust will make use of free tools provided by accredited organisations to aid in this process. Issues found as a result of this monitoring should be acted on immediately and appropriately.

4.5.2 Where possible, automated vulnerability scans should be performed on all networked devices, with issues being managed or remedied within an acceptable time frame.

4.5.3 IT Managers are responsible for ensuring the Trusts IT Systems and Network do not pose an unacceptable security risk to the organisation. This policy should be viewed as the minimum requirements for protecting the Trusts Systems, Network and its Data. Where systems pose a risk this must be raised in the KCHFT risk register.

4.5.4 CareCERTs will also represent part of the Trusts Vulnerability Management Strategy, as will vulnerability scans performed by external auditors and other third parties to identify where vulnerabilities present a risk to the Trust.

4.5.5 The trust will also make use of Penetration tests performed by accredited companies to assess both internal and external IT systems, and high value assets.

4.6 Configuration and Change Control

4.6.1 The Trust will have a robust process for effecting and logging changes made to the IT Systems and Network. All Teams must use the Trusts Request For Change Process which is available to all required members of the IT Teams. All changes will be logged, and approved using the Request for Change (RFC) document which is available to all IT Teams.

4.6.2 Adequate testing must be performed before deployment to live environment. Test reports should be attached where possible, and a reliable back-out plan must be in place.

4.6.3 Testing facilities will be used for all new systems. Test/development and live/production environments should be separated as much as possible.

4.6.4 IT Teams will review the RFC log at least 12 monthly to ensure any temporary changes no longer required are reverted or removed.

4.7 Disable unnecessary peripheral devices and removable media access

4.7.1 USB access is blocked by default on the Trusts network; any exceptions to this must go through the trusts approval process via the IT Service Centre.

4.7.2 Removable media usage will be continuously logged, and audited on a weekly basis.

4.7.3 An auditable list will be kept of any device exceptions required.

4.7.4 IT Teams will work towards a “disable by default” standard and with required devices and peripherals excluded via an allow list approach.

4.8 Removable media

4.8.1 Removable media gives the capability of copying, storing and transferring large amounts of data, which could be potentially sensitive. USBs can be easily lost or stolen; they retain information even after deletion, and also have the ability to introduce Malware into the Trusts network. This includes any removable storage in digital image or film cameras, and mobile devices.

4.8.2 If unencrypted removable media is to be taken off site, staff MUST complete the Risk Assessment for Transportation and Storage of Personal Confidential or Business Sensitive Information Off-site prior to the information being removed.

4.8.3 Staff are not permitted to connect personal mobile devices to Trust provided equipment (This includes for charging purposes)

4.8.4 Only Trust approved devices are permitted on the Trusts network, and non-approved devices will be blocked by default. The Trust will provide users with a password protected and encrypted device as an alternative. This device will meet all required NHS Digital removable media standards.

4.8.5 If there is a genuine need for the use of non-KCHFT provided media devices to allow a user to perform their job role requirements, and an encrypted device is not financially viable or practical, then the device will need to be scanned before being introduced to the network and the need justified and approved by both line manager and responsible IT manager.

4.8.6 The Trust will maintain a list of approved devices which are allowed on the network.

4.8.7 The Trust will work towards a “block by default” policy and controls for all USB media on the Trust network.

4.8.8 Removable media will be automatically scanned whenever it is connected to the Trusts network.

4.8.9 If media is being brought into the organisation from an unknown source then it will be scanned on a dedicated standalone PC before being permitted for use on the Trusts network.

4.8.10 The Trust will formerly issue removable media to users on request who will be responsible for its use and safe-keeping.

4.8.11 All removable media will be encrypted by default, and will meet current encryption standards required by NHS Digital and the Network and Information Security Directive (NIS).

4.8.12 If for any reason the removable media device cannot be encrypted then sufficient physical/administrative controls must be in place to ensure the security of the data contained on the device. There must also be a process to make “chain of custody” auditable, with a signing in and out procedure, and a local standard operating procedure must be available to staff.

4.9 Application Control

4.9.1 Wherever possible application allow lists will be but in place across all endpoints, and devices. The trust will work towards a “default deny” policy.

4.9.2 All new applications including those which are not included in the standard OS base image/install are to be tested and approved via RFC process before being rolled out for use in live environment.

4.10 Email

4.10.1 Staff must use the NHS.net email address provided to them for all email communication.

4.10.2 Staff must use the provided email system in accordance with the *Use of Email SOP* which is available on flo.

4.11 Printing and Scanning

4.11.1 Where possible the Trust will implement a system which requires authentication to retrieve print jobs. This will be linked to Active Directory permissions and require an identity token.

4.11.3 Printing from home is permitted however all KCHFT IG and data protection policies still apply and must be followed if PII or sensitive business data is involved.

4.11.4 Important information regarding printing from home is contained in the *Home, Remote and Mobile Working SOP* available on flo.

4.12 Cryptographic Controls

4.12.1 Appropriate cryptographic controls will be used to ensure the integrity, confidentiality and availability of the communication, processing and storage of confidential information.

4.12.2 Emphasis is placed upon external communications, but the provisions also apply equally to internal communications where there may be a risk of compromising confidentiality.

4.12.3 All Cryptography used within the Trust must meet the standards required by NHS Digital, the NIS directive and Law.

4.13 Key Management

4.13.1 Adequate measures shall be taken to minimise the risk of loss or compromise of cryptographic keys, which shall include:

a) defined activation and deactivation dates so that keys can only be used for a limited period;
b) logging and auditing of key management related activities (e.g. creation, destruction and archiving);
c) procedures for the revocation of keys (e.g. on staff termination or key compromised);
d) Procedures shall be in place for the production of cryptographic keys in the event of an authorised person making a written request in accordance with the Regulation of Investigatory Powers Act 2000.

4.14 System Ownership

4.14.1 Each of the Trust' systems and applications which interact with or contain PII will be owned and be the responsibility of a specified Systems Manager or IAO whose responsibilities will include ensuring compliance with this Policy, ensuring the appropriate use of the equipment, troubleshooting and maintenance.

4.14.2 All information possessed by or used by a particular organisational unit or service must have a designated owner who is responsible for determining appropriate sensitivity classifications and criticality ratings, making decisions about who can access the information, and ensuring that appropriate controls are utilised in the storage, handling, distribution, and regular usage of information.

4.14.3 Each KCHFT IT system will be owned and be the responsibility of a specified system manager (IAO) whose responsibilities will include ensuring compliance with this Policy, ensuring the appropriate use of the equipment, troubleshooting and maintenance. Application managers/owners will also be responsible for user account audits where accounts are not centrally controlled by the KCHFT Active Directory.

4.14.2 Please refer to section 2.9 for the responsibilities of Information Asset Owners (IAOs) and section 2.8 for the responsibilities of system managers

4.14.3 The IT Service is not responsible for determining the sensitivity of any clinical data contained on the system.

4.14.4 Each individual service is responsible for the management of each application or system they use. The only exceptions to this are the systems in use trust-wide, (For example NHS Mail, Teams, RIO) or if formerly agreed with IT.

4.15 Asset Management

4.15.1 The Trust will have an asset management solution to ensure an up to date inventory of all active IT assets. Different hardware may be recorded on separate systems to form the Trusts inventory.

4.15.2 The purpose of the asset inventory is:

a) To identify the location of all Trust IT assets;
b) To identify and authorise the use to which such assets are put;
c) To manage capital charges on physical assets.

4.15.3 Each IT Team is responsible for the inventory of the assets under their control, and should perform an internal audit of assets at least annually.

4.15.4 See section 12.0 Physical and Environmental Security for asset disposal.

4.16 Asset Tags

4.16.1 Staff should be aware of the origin of the IT equipment being used to fulfil the Trusts activities. All IT equipment which has been purchased must have a Trust asset tag assigned to it and recorded within the IT asset management system. Where practical the asset tag will be physically visible on the equipment stipulating that it is the property of KCHFT.

5.0 NETWORK SECURITY

5.0.1 The Trusts network needs to be protected from both internal and external threats. Failure to implement appropriate security controls, or poor network design and architecture can result in exploitation of the network. This may result in damage to

critical infrastructure, inability to deliver front-line services, loss of patient or staff confidence. It may also allow access to, and the ability to remove confidential systems hosting sensitive information resulting in heavy fines loss of patient confidence, and damage to the Trusts image. It could also result in the Trust losing complete control of its own network and resources, and also defacement of public facing websites.

5.1 Network Perimeter

5.1.1 The Trust will use systems which control and manage all inbound and outbound network connections, and deploy technical controls which can scan for malicious content. Access to ports, protocols, and applications should be managed by inspecting all network traffic at the perimeter to block anything which is malicious.

5.1.2 Any connections to external networks and systems must have documented and approved IT Security Policies, SOPs or clear documentation.

5.1.3 The Cyber Security Specialist and/or IT Infrastructure Manager must approve all connections to external networks and systems before they commence operation.

5.2 Firewalls

5.2.1 The Trust will use firewalls to create buffer zones between the internet, and other untrusted networks and the Trusts network. The firewalls should work on a default “deny” ruleset with an allow list applied for authorised traffic, ports, protocols and applications, including their ability to communicate across the network boundary.

5.2.2 Changes to Firewall configuration must come through the Trusts RFC (Request For Change) process.

5.2.3 All firewalls and perimeter appliances should have regular audits to ensure removal of unused rules and configuration integrity.

5.2.4 Access to the firewalls will be limited to only necessary personnel, and remote administration should only ever be performed over a secure, encrypted connection. They must not be accessible via the internet.

5.3 Operating Procedures

5.3.1 IT operating procedures for the day to day secure operation of the network must be in place, and be documented and monitored. Performance reports should be produced when required and submitted to IT Systems/infrastructure manager as applicable.

5.3.2 Standard operating procedures (SOP’s) for all staff will be in place to ensure all staff understands how to work securely within the trust.

5.4 Preventing malicious traffic at the perimeter

5.4.1 All traffic travelling in and out of the Trusts network should be examined by malware and reputational scanning. These will ideally be different from the systems used internally (For example; the computer based Anti-Virus) to provide some additional protection in depth.

5.4.2 See Section **9.0 Malware Prevention** for more information.

5.5 Protecting the internal network

5.5.1 There should be no direct routing between the internet and the internal network to limit exposure of attack from the internet.

5.5.2 Internal network traffic should also be monitored to detect attempted attacks, or network intrusions.

5.5.3 A DMZ should be used for internet facing services to ensure separation from the internal corporate network. See below for network segmentation.

5.6 Network segmentation

5.6.1 Critical Systems, and data centres should be isolated from other networks. Internet facing services should be placed in a DMZ where possible to better protect internal networks from compromise through “Lateral Movement”.

5.6.2 Where end of life critical infrastructure and unsupported Operating Systems cannot be removed, they must be separated either physically or logically from the Trusts network, and all other appropriate steps must be taken to mitigate or reduce the risk of these devices as much as possible, with the risk logged in the KCHFT Risk Register.

5.6.3 IT Teams must have a SOP for any systems which fall under point 5.6.2.

5.6.4 Any Internet Of Things (IOT) device must be separated either physically or logically from the Trusts network, and all other appropriate steps must be taken to mitigate or reduce the risk presented by these devices as much as possible.

5.6.5 All configured networks must be fully documented, and undergo regular reviews to ensure they are kept up to date.

5.7 Wireless Access

5.7.1 All wireless Access Points will be appropriately secured, and only “known” devices should be allowed to connect to the Trusts network.

5.7.2 Wireless usage will be monitored for excessive usage or violations of the Trusts Cyber, Network and Information Security Policy.

5.7.3 Where access is provided to a “Guest” wireless network a login capture portal will be used to register users, only logging any information as required by law.

5.7.4 Patient WiFi services will be separated from the Trust network by Virtual Local Area Network (VLAN) and by a Firewall.

5.7.5 Staff are not permitted to access and use the Patient Wireless network.

5.8 Exception Handling and Disclosure of Sensitive information

5.8.1 Error messages on public facing services should be configured to only show generic information, as some error messages can provide information which would aid an attacker attempting to compromise the Trusts Network.

5.9 Network Monitoring

5.9.1 Where possible the Trust will deploy Network Intrusion Detection (NIDS) and Network Intrusion Prevention Systems (NIPS) which will monitor all traffic for anomalies or signs of malicious traffic. Alerts should be generated by the systems which are monitored by the appropriate responsible IT Team.

5.9.1 Logging will also be enabled and monitored for high value systems. See 10.0 Monitoring

5.10 Web filtering

5.10.1 The IT Department or their service providers will block access to Internet websites and protocols that are deemed inappropriate for the Trust.

5.10.4 All authorised changes to web and protocol filtering rules will be done via Change Control Procedures.

5.10.7 Employees have a responsibility to ensure they use the Internet and Intranet in a professional, ethical and lawful way at all times.

5.11 Auditing

5.11.1 The Trusts policy, its implementation, and systems will be subject to periodic review by both internal and external auditors, the recommendations from which will normally be implemented unless specific dispensation is given at organisational management level. Any major security incident is liable to be referred to the auditors for investigation and /or the Counter Fraud Team for further investigation.

5.11.2 The Trust will engage with external organisations to undergo periodic technical testing of both internal and external IT systems.

5.12 Maintenance Contracts and Service Level Agreements

5.12.1 All Service Level Agreements (SLA's) must stipulate that maintenance contracts are maintained and periodically reviewed for all equipment.

6.0 ACCESS CONTROL

6.0.1 The control of access to systems is critically important to protecting the confidentiality, integrity and availability of our information. Access to systems may only be granted to users on a least privilege basis and shall be subject to appropriate identification, authentication and ongoing review including removal of access when a user changes role or ceases to be employed by the Trust.

6.1 User Account Management

6.1.2 The Trust will adopt a “least privilege” permissions model ensuring both Administrative and standard user accounts should only have the permissions they require to fulfil their job role and no more.

6.1.3 Standard user accounts should not be able to install/uninstall software, or disable running services. This will be managed by the use of Active Directory Groups and related Active Directory Group Policies.

6.1.4 Temporary elevated privileges can be granted on a case by case basis; however these must be logged appropriately, approved by a responsible IT Manager, and then removed when the need is no longer required.

6.1.5 Administrative and elevated privilege accounts are to not to be used as a standard user account or to browse the internet, use email, or any other function not related to the tasks the account has been provisioned for.

6.1.6 The Trust will have a robust set of processes in place to monitor User accounts from creation to deletion. Each part of the process should be auditable, providing the ability across Teams and departments to cross reference and identify anomalies. A leaver’s process should be in place to ensure all leavers accounts are disabled across all systems.

6.1.7 The Trust will monitor all user activity, particularly access to sensitive information, email and internet use, logon activity, and the use of privileged accounts.

6.1.8 Active Directory (AD) permissions will be regularly audited to prevent “privilege creep”. (See GLOSSARY AND ABBREVIATIONS)

6.1.9 New starters shall only be granted access to systems as requested by HR. The procedure for granting access to new systems is set out in the IT AD Account Creation Process.

6.1.10 User access rights shall only be amended as requested by HR or the user’s line manager. The procedure for granting access to new systems is set out in the *Starters, Leavers and Movers SOP* available to all IT Teams.

6.1.11 Access to systems shall be disabled or deleted when a user ceases to be employed by the Trust. The procedure to be followed for disabling or deleting systems is set out in the IT Leaver Process which is a web form available on Top Desk via the IT Service Centre. Line Managers MUST ensure all IT accounts are removed or disabled when a staff member leaves the organisation.

6.1.12 Standard access rights shall be reviewed at least annually and privileged access rights shall be reviewed at least every three months. Access rights shall be removed if it is identified that access or privileged access is not strictly required for the user’s job role.

6.1.13 Any active user accounts not accessed for at least three months shall be reviewed and shall be disabled unless there is a documented business justification for keeping the account enabled which has been approved by a senior IT Manager.

6.1.14 Access to Clinical Systems will be protected by 2 Factor Authentication wherever possible. Smart Cards will be managed centrally by responsible IT Team. (See Registration Authority Policy)

6.1.15 Access to certain systems may require specific authorisation from the Caldicott Guardian or delegated authority.

6.1.16 Information Asset Owners are ultimately responsible for maintaining all starters and leavers requests to ensure that the integrity of the system is maintained.

6.1.17 The user access management procedures set out in this policy shall be reviewed at least annually, with review outcome recorded.

6.1.18 All user accounts must be created/changed and removed in accordance with the following internal IT SOPs

a) IT AD Account Creation Process.
b) IT AD Account Rename Process.
c) IT Leavers Process.
d) IT Shared Drive (Permissions) Access Process.

6.2 Passwords

6.2.1 The use and management of suitable passwords is fundamental to the security of our systems and information. Systems shall be configured to enforce the minimum password standards set out in this policy.

6.2.2 Complex passwords, meeting the password standard set out in this policy, shall be used to control and limit access to the Trust's information systems to authorised users only.

6.2.3 Password Standard for all systems shall be configured to require passwords that meet the following criteria:

- Longer than 8 characters

6.2.4 They must also contain three of these four complexity requirements.

- Contain uppercase letters (A-Z)
- Contain lowercase letters (a-z)
- Numbers (0-9)
- Special characters (*&^%$£"!)

6.2.5 Users shall be required to create unique passwords for each system to which they require access.

6.2.6 Passwords for systems should be unique and complex. Common phrases and names must be avoided.

6.2.7 Where a password is created by a system administrator and shared with a user for use when first logging in, the password shall be randomly generated, and the system shall be configured to require the user to change the password at first log-in.

6.2.8 Domain User Password Resets shall require validation of the identity of the user. Once the user's identity has been validated, a randomly generated temporary password shall be issued to the user and domain joined systems shall require the user to change the password at next log-in. See the following internal IT SOPs;

a) AD NHS.net and Vismo Password Reset Process.
b) AD Password reset Process.

6.2.9 When a user requires their password to be reset, they must follow the steps below:

- Ring the Service Desk to raise a ticket for a password reset.
- Provide the requested information about the account which requires a reset.
- Validate your identity with the Service Desk.
- Use the password you're provided with immediately.
- Create a password in accordance with the password standard detailed within this document.

6.2.10 The way in which a user will validate their identity when conducting a password reset is by answering security questions, these will be set up as part of induction and the account creation process. If the security questions cannot be answered, a senior member of the user's department will verify their identity.

6.2.11 Password Lockout

Systems shall be configured to lockout users for 30 minutes after 5 unsuccessful attempts to access an account. Users locked out of a system shall be required to follow password reset procedure for the system.

6.2.12 Password Security

Users shall ensure that all efforts are made to keep passwords confidential, the following list is not exhaustive but will aid in preventing disclosure accidentally:

- Passwords should not be written down on paper. Password managers may be used however a strong password must be used to prevent unauthorised access.
- User account passwords must never be shared with other users or administrators.
- If there is any reason to suspect a password is compromised, this must be reported and changed immediately using the password reset procedure for the applicable system.

6.3 Remote Access

6.3.1 Remote working is an integral part of how the organisation functions as a community trust, however remote access will be tightly controlled and monitored.

6.3.2 Remote Access into the Trusts network will require the use of 2 Factor Authentication (2FA) and VPN which will be centrally managed by responsible IT Team. This will be auditable and log user access.

6.3.3 Users can request VPN access by completing the "VPN Token Request Form" which is available through the IT Service Desk Self-Service Portal.

6.3.4 VPN tokens will be centrally managed by responsible IT Team to ensure leavers have remote access removed/disabled. (See 6.1 User Account Management)

6.3.5 Access will only be granted after completion of the Trusts registration procedure.

6.4 Third Party Access

6.4.1 Third Party Access to the Network will be based on a formal contract that satisfies all NHS Security conditions, and all the Trusts Security requirements.

6.4.2 No external agency (NHS or otherwise) will be given access to any of The Trust's networks, assets, endpoints, or devices unless that body has been formally authorised by the Cyber Security Specialist in conjunction with the IT Manager to have access and/or to exchange data. All non-NHS agencies will be required to sign security and confidentiality agreements with The Trust, and meet a standard for cyber security which will be specified in the contract with the supplier

6.4.3 Access to the network must be auditable, with regular checks of user accounts for Third Parties to assess access level and permissions.

6.4.4 Third Party Active Directory Accounts are disabled by default unless offering 24 hour support to critical infrastructure.

6.4.5 Each supplier requiring remote access will be required, before access is granted, to provide a written commitment to maintain confidentiality of data and information and only use qualified representatives.

6.4.6 Request for remote access will be authorised by responsible IT Manager and/or Cyber Security Specialist, who will only authorise the connection when the business need has been satisfied. The connection will be physically broken when the fault is fixed/supplier ends his session, and any installed support software will be removed immediately.

6.4.7 Suppliers of central systems/software commonly request to have remote access to such systems to investigate/fix faults. The Trust will permit such access and activity will be monitored.

6.4.8 All Third Party access to the network must be logged, and the access confirmed as removed when no longer required.

6.4.9 Third Party Access must be periodically checked, and access removed where no longer required, or disabled if more appropriate.

6.4.10 All Third Parties will need to sign the appropriate section of the "Confidentiality Code of Conduct" which can be found on flo.

6.4.11 Any remote support software installed for the purpose of support must be completely removed or uninstalled at the end of every support session.

6.4.12 Third Parties should connect via Trust provided appliances. Third Parties are not permitted to connect their own equipment to the Trusts network.

6.4.13 All Third Party Access, including remote access will be chaperoned by appropriate IT Team member.

6.4.14 For third party remote access requirements and account creation see - SOP - Third Party Open Access and Remote Connection_FINAL

6.5 Privileged Accounts

6.5.1 The Trust will strictly control the granting of privileged and highly privileged accounts for example local, and Domain Administrators,

6.5.3 Users of privileged accounts will have additional training if required.

6.5.4 Privileged accounts will be subject to closer monitoring.

6.55 The minimum level of permissions will be applied in all cases where elevated privileges are requested, including service accounts.

6.5.6 Privileged access to systems shall only be granted where approved in accordance with the Trust's IT change management process.

6.5.7 Two-factor authentication is required for privileged account access on all systems where available.

6.5.8 Privileged accounts MUST only be used where administrative permissions are required and users must use their standard user accounts for all other activities including email and internet access.

6.5.9 Any individual working for, or on behalf of the Trust that is provisioned with an account with elevated privileges most comply with the same standards.

6.6 Employment

6.6.1 Users will need to complete the Smart Card Registration Form before a Smart Card can be issued. This form will be provided on induction if required and is also available on flo.

6.6.2 Terms and conditions of employment will include the employees' responsibility for information security and require an employee to sign a Confidentiality Code of Conduct. Job descriptions will include the appropriate security roles and responsibilities specified in this policy.

6.6.3 Recruitment to specific roles managing Information Management/Technology Systems will be subject to verification checks to include validating their technical ability, academic and professional qualifications and taking up references.

6.6.4 Bank and temporary staff should be suitably obtained from a reputable source which meets all current standards and requirements.

6.6.5 Sufficient checks need to be carried out to ensure Bank and Temporary staff are both vetted and qualified before being granted access to the KCHFT network and/or systems.

6.6.6 RA Policy is available here - Registration Authority Policy

6.7 Network Drives

6.7.1 The H: drive is for personal data you do not want to share with your colleagues and it is only accessible by yourself: e.g. appraisal prep, expenses, helpful notes, or a working area before a document is ready to be shared. Do not store patient data in this location. No personal data relating to patients, or staff members should be held in this drive.

6.7.2 The K: drive is for shared/departmental data, anything your colleagues would also require access to in your absence, e.g. standard operating procedures, manuals, patient data. You can request restricted access to documents on the K drive

7.0 USER SECURITY POLICY

7.0.1 The Trust will have a Data Security and Protection Policy which will be easily available on Flo, which staff are required to read as part of their local induction.

7.0.2 Please remember;

- Confidential information relating to staff, patients or the Trust must not be made available on the Internet in any way, including via internet newsgroups, social media or website discussion groups.

- The browsing of infected or malicious websites represents one of the main threats; staff should only browse known and trusted websites and only in line with their work related activities.

- The use of streaming sites is forbidden unless there is a genuine work requirement. Streaming videos, music or radio is a breach of this policy unless express permission has been granted by responsible IT Manager or Cyber Security Specialist. There are licencing issues you may not be aware of which could result in the trust receiving a fine.

- If working remotely (both wireless and wired) from either your home or anywhere else, then users should always connect to the VPN even if accessing websites which don't require it, and not working from the network drives. (The VPN not only provides access to the network, it also adds an additional layer of security for any data while in transit.

- Any smart device such as google home or Amazon Alexa, MUST be switched off if you are receiving any phone or video calls.

- Information obtained from the internet may not be accurate. Therefore, the user must check the accuracy, adequacy, or completeness of any such information. KCHFT recommends only using recognised organisations such as such as NICE, WHO, DoH, NHSX, NHS Digital/England. Furthermore, it is everyone's responsibility when using information obtained from the internet, to be aware of copyrighted material in accordance with the permission granted by the publisher.

- Users must inform the IT Service Centre of any virus found or suspected and raise a Datix incident.

- You must not attempt to install any mobile app, application, or software of any kind on any trust IT asset. Please complete the request forms available on the IT Service Centre system.

- You must not connect ANY non-KCHFT device to your laptop, desktop, phone or tablet. This includes smart phones, external drives and printers.

- You must not implement any new IT system either on premise, or cloud based without first contacting the IT Project team. This includes systems where PII will **not** be used. All systems must be assessed by IT prior to use, and DPIA's must be completed where required.

- See Section 6.2 for password guidance.

7.1 Induction Process

7.1.1 New Users (including Contractors and Third Parties) will be made aware of their personal responsibilities to comply with the appropriate Trust policies.

7.1.2 All terms and conditions of their employment will be formerly acknowledged and retrained to support any necessary action is the case of an issue.

7.1.3 All employees, permanent, temporary, and relevant third party users shall receive appropriate training and regular updates on the Trusts policies and procedures.

7.1.4 Authorised users of Information Management/Technology Systems, including clinical systems shall receive appropriate training and are not permitted to access live systems until training has been completed.

7.1.5 Training will be audited by an external organisation.

7.2 User Education and Awareness

7.2.1 The Trust will ensure users are aware of and have easy access to the Trusts policies around Cyber Security, and that they are also aware of their personal responsibility to adhere to these policies.

7.2.2 The Trust will also provide easy access for employees to the Cyber Security Specialist so they are able to get quick advice and answers to questions.

7.2.3 The Trust will have mandatory Cyber Security training for all staff.

7.2.4 The Trust will ensure that Cyber Security Training is refreshed and updated in line with current trends, and Users will be assessed on a 12 monthly basis as a minimum requirement and will be reviewed at appraisals. Training will be audited by an external organisation.

7.2.5 The Cyber Security Specialist will ensure current risks are communicated across the Trust to front-line staff as well as the IT Technical Teams, and senior stakeholders.

7.2.6 The Cyber Security Specialist should be directly accessible to all staff should they require advice regarding Cyber Security.

7.2.7 Additional training will be provided for any staff member who requests it.

7.2.8 Staff in Security roles will be encouraged to develop and validate their skills through certification or recognised schemes.

7.2.9 The Trust will provide specialist training where required for specialist roles.

7.3 Monitoring Training Compliance and Effectiveness

7.3.1 The Trust will have mechanisms in place to enable it to assess compliance level and effectiveness of Cyber Awareness Training.

7.4 Disciplinary Process

7.4.1 Any member of staff in breach of information security contained within this policy or other supporting policies may be subject to the organisations disciplinary procedure and be dismissed from employment if deemed appropriate. Please see section 5.6 of the Disciplinary Policy (Misuse of Information Technology)

7.4.2 The Trust will provide guidelines for staff regarding acceptable use of the Trusts Network and Systems.

7.5 Staff Owned Equipment

7.5.1 The use and storage of Trust person identifiable or confidential data on staff owned equipment is strictly forbidden.

7.5.2 Staff must not use personally owned computers for work related activities. For prevention of viruses and related security risks, staff must not connect any personally owned devices to the Trust network. Personally owned USB devices or other removal media should not be used. Personal devices must not be connected to Trust-owned equipment.

7.6 Personal Mobile Devices

7.6.1 The Trust does not support a Bring Your Own Device (BYOD) environment. Users are not permitted to connect any personal devices to the Trust network or access any business system via a personal device. The only exceptions to this will be listed directly below in this policy below, with links to relevant SOPs.

7.6.2 Flo mobile app – *Flo mobile app SOP* available on flo.

7.7 Video Consultations

7.7.1 Video consultations are permitted however there are strict guidelines which must be adhered to and any deviation from this is prohibited.

7.7.2 See the *Video Conferencing and Consultations SOP* on flo.

7.8 Instant Messaging

7.8.1 In some cases the use of Instant Messaging (IM) is permitted however there are strict guidelines which must be adhered to and any deviation from this is prohibited.

7.8.2 See the *Instant Messaging SOP* on flo.

7.9 Smart and voice activated devices.

7.9.1 Voice activated smart devices such as Alexa, Google Home, Nest Hubs are not permitted in KCHFT buildings.

7.9.2 If working from home then any voice enabled smart devices should be switched off or disabled for the duration of the work day if you are to be receiving calls which may contain PII or other sensitive data.

7.9.1 Further information on smart devices is covered within the *Remote, Home and Mobile Working SOP* which is available on flo.

7.10 Allowing others to use your computer or login credentials

7.10.1 Allowing another person to use your login or smartcard to access data, systems or for any other reason is a breach of policy. You may be subject to disciplinary procedures and it may constitute an offence under the Computer Misuse Act 1990.

7.10.2 You must take all reasonable measures to protect computers and devices being accessed unlawfully, this includes preventing people from entering buildings due to doors being propped open, leaving your mobile device/laptop in your car overnight, or unattended while being logged-in when working from home or remotely.

7.10.3 When working from home don't be tempted to let someone login to a website, or check Facebook for example using your laptop or other KCHFT device and login. You are responsible for anything that occurs using your login. This policy applies regardless of the working location. See the *Home, Remote and Mobile Working SOP on flo.*

7.10.4 For guidance relating to malware prevention see section 9.1 Anti-Malware Guide for users

8.0 INCIDENT REPORTING AND MANAGEMENT

8.0.1 Security incidents will inevitably occur, and these will vary in the level of seriousness and impact. All incidents need to be managed effectively through a robust process from discovery to lessons learned.

8.1 Cyber security incidents

8.1.1 All incidents should be recorded via the Trusts centralised incident reporting system Datix, and investigated by appropriate managers.

8.1.2 For disaster recovery and business continuity plans see the Trusts IT BCDR Plan which is available from the IT infrastructure managers.

8.1.3 For Cyber incident response please see CIR Plan available via the Cyber Security Specialist or IT infrastructure managers.

8.1.4 The Trust will promote a cyber incident reporting culture which empowers staff to voice concerns regarding poor practice or security concerns.

8.1.5 Staff will be able to contact the Cyber Security Specialist directly to voice any concerns they may have. Contact details published on Flo.

8.2 Specialist Training

8.2.1 The Trust will either provide support for relevant staff members to complete specialist training, or use a specialist third party provider for serious incidents where this is considered to be appropriate.

8.3 Data Recovery Capability

8.3.1 The Trust will have suitable Data Recovery Capability in place at the appropriate level in respect to the legal and business requirement. The main elements of this process will include:

a) identification of critical information assets and computer systems
b) identification and prioritisation of key users/user areas
c) agreement with users to identify disaster scenarios and what levels of business continuity are required
d) identification of areas of greatest vulnerability based on risk assessment
e) mitigation of risks by developing resilience
f) developing, documenting and testing business continuity plans identifying tasks, agreeing responsibilities and defining priorities

8.3.2 All IT Teams are responsible for the data recovery ability of their respective systems.

8.3.3 Each IT Team will have a SOP to document all backups in place and associated settings and schedules, which will form part of the internal IT teams SOP library held by IT centrally.

8.3.9 The BCDRP will be regularly updated to reflect the current location and status of the Trusts backups, information on systems and documentation including full recovery plan and contact information for responsible team members.

8.3.10 The Trust will also ensure adequate training is provided to ensure the organisations ability to recover effectively after a serious incident.

8.4 Testing Incident Response

8.4.1 The Trusts Emergency Preparedness, Resilience and Response Team will regularly test the incident response plan, all necessary staff will be involved and a written report on lessons learned produced. The BCDR Plan will then be updated to reflect the outcome of the test, and make any improvements or changes as required.

8.5 Post Incident Evidence

8.5.1 The Trust will make every effort to preserve evidence post incident. The Trust will have a 'Chain of Custody' process in place so all relevant staff are aware of their responsibilities with regards to evidence.

8.5.2 In the event that evidence needs to be seized or gathered, staff are to follow the process outlined in the *IT Evidence Seizure SOP* available on flo.

8.6 Incident Review

8.6.1 The Trust will investigate all Security incidents and each will be reviewed for lessons learned. Any improvements that can be made as a result of the investigation will be put forward for further review by appropriate groups and implemented where approved.

8.7 Criminal Incidents

8.7.1 The Trust will report Cyber Crime and breaches of the law to the appropriate law enforcement agency. (In the case of Cyber Crime **https://www.actionfraud.police.uk**)

8.9 Incident Near-misses

8.9.1 All individuals are responsible for recording all actual and near miss security incidents involving any aspect of information governance and are to be reported in line with the Trusts incident policy.

8.10 Ransomware

8.10.1 Any instance where Ransomware is found or suspected must be reported immediately without fail to either the Service Desk or Cyber Security Specialist. Due to the incredibly time-sensitive nature of this kind of attack, even if out of hours IT on-call must be notified. The details are available on Flo.

9.0 MALWARE PREVENTION

9.0.1 Malware infections pose a large risk to the Trust and could result in the complete failure of the entire Trust network or the removal of sensitive data from clinical systems. Malware is constantly evolving and so a dynamic approach to Malware prevention is required. The main risks are;

- Email – Malicious links and attachments are still the number one attack vector for all businesses.
- Web Browsing – Users browse to malicious sites, or genuine sites which have had malicious code injected into them. Malicious ads or links are the main risk, as is downloading malicious software from the internet.
- Web Services – Users access social media or personal email accounts which present a risk of personal accounts being used an attack vector against the Trusts network.
- Removable Media – Malware can be introduced to the Trusts network and systems by personal devices carrying malware transported for home PCs. This also includes mobile devices which if infected can also infect the Trusts network when connected for charging purposes.

9.1 Anti-Malware Guide for users

9.1.1 Users must not attempt to prevent Anti-Malware updates or patches being applied to their workstation.

9.1.2 Users must not disable the Anti-Malware software on their workstation.

9.1.3 Users must not attempt to prevent the system from running automatic updates.

9.1.4 Users must restart their systems at least once a week.. This allows the Anti-Virus to perform enhanced removal of malicious software where required, and the installation of system and application updates.

9.1.5 Users must connect to their local network at least once every 2 weeks, and preferably once per week to allow Anti-Malware databases to update.

9.1.6 Users who have permission to install their own software on their workstation must ensure that this software is kept updated, and is removed when no longer required.

9.1.7 Users should notify the IT Helpdesk or Cyber Security Specialist immediately if they suspect a virus is present on any device connected to the network.

9.7.2 All occurrences of viruses will be dealt with as a high priority to ensure that the spread of the virus, malware or ransomware is kept to an absolute minimum.

9.1.8 Users will only use Trust approved removable media on Trust devices, and computers

9.1.9 The browsing of infected or malicious websites represents one of the main threats; staff should only browse known and trusted websites and only in line with their work related activities.

9.2 Data Scanning

9.2.1 The Trust will make best efforts to scan all data at the point of entry, whether that be on external drives connecting to a Trust machine to copy data, or at the network perimeter when data enters or leaves the network.

9.2.2 No newly acquired disks, magnetic media, or CDs, should be loaded unless they have previously been virus checked by a locally installed virus-checking package. E-mail attachments must be checked before they are opened. (All emails are scanned by nhs.net before being delivered to a Trust email address)

10.0 MONITORING

10.0.1 Monitoring provides the Trust with the means to identify unusual behaviour on the network, and diagnose issues more efficiently, and provide a baseline with which to compare suspected issues, increasing the likelihood of detecting an attack. It also allows a level of auditing and the ability to establish accountability in some cases where required.

10.1 Event types and systems

10.1.1 The Trust will where possible monitor all systems with both signature based capabilities for known attacks, and a heuristic based system to detect unusual system behaviour. The strategy will include the below;

- **Network traffic.** This will be monitored for unusual network traffic and connections, and have alerts setup to warn of certain behaviour or events when they occur.
- **User Activity.** All aspects of user behaviour will be monitored. This includes USB usage, browsing habits and account activity information.
- **Centralised Logging.** The Trust will make best efforts to centralise as much of the logging and monitoring as possible.
- **Logging Solution.** This will be regularly reviewed to ensure the correct data is being collected so relevant information is not being lost in excessive, irrelevant data.

10.2 Email monitoring

10.2.1 All email usage and web access is monitored for the following reasons:

- providing evidence of communications;
- ensuring that the organisation's business procedures, policies and contracts with employees are adhered to;
- complying with any legal obligations (e.g. The Freedom of Information Act and Data Protection Act, GDPR);
- monitoring standards of service, employee performance, and for employee training;
- preventing or detecting unauthorised use of KCHFT systems for criminal activities; and
- maintaining the effective operation of the Organisation's communication systems

10.3 Internet Use (Web Browsing)

10.3.1 The IT Department will monitor (directly or by their service providers) Internet use from all computers and devices connected to the corporate network.

10.3.2 For all traffic, the monitoring system will record the user, the date, the time, the protocol, the destination site or server initiating the traffic.

10.3.3 Internet usage is monitored from all trust IT assets/computers even when they are not connected to the NHS (N3/COIN) network. The Trust has an internet facing proxy server which records activity on trust computers when they are not connected to the corporate network.

10.3.4 Appropriate IT staff will monitor KCHFT internet access using the monitoring and reporting tool.

10.3.5 Internet usage reports that identify specific users, sites, teams, or devices will only be made available upon a request from the Human Resources department, Line Manager or Information Governance team.

10.3.6 Frequent monitoring from the IT team will also flag excessive usage of prohibited sites to line management or HR for further investigation.

10.3.7 Information regarding suspected criminal activities may be passed to the appropriate authorities if discovered. Staff may be subject to the Disciplinary Policy.

10.4 System Logs and Auditing

10.4.1 Logging IT activity is vital to the incident response, and IT forensic ability of the trust.

10.4.2 The trust will log as much activity as is reasonably possible based on system integration, and storage availability.

10.4.3 The most high value systems and alerts will take priority, and the most critical will be monitored by responsible IT Teams.

10.4.4 Logs should be kept for a minimum of 6 months, but ideally for longer for the most critical logs to allow historic forensic work.

10.4.5 Access to any audit log system will be strictly controlled to preserve the integrity of the content.

11.0 HOME AND REMOTE WORKING

11.0.1 As a community trust home and mobile working is widely undertaken throughout the organisation. Home and remote working are subject to the same policies and, technical controls as if working from either a KCHFT or partner organisation location.

11.0.2 A home or remote working location should be treated in exactly the same way as a “work” location, and if you cannot meet the requirements then these elements of working should not be carried out until it is safe to do so

11.0.3 This includes but not limited to;

- Screen privacy
- Password secrecy
- Physical device security
- Printing
- Internet browsing
- Email use
- Accessing work systems
- USB devices and external storage
- Data access and copying
- Video conferencing and consultations
- Phone calls
- Adhering to National Data Guardian Standards and Caldicott principles.

11.0.4 Further information and guidance is available via the *Home, Remote and Mobile Working SOP,* and the “Working from Home Toolkit” on Flo.

11.1 Mobile devices

11.1.1 As a community trust mobile devices are widely used throughout the organisation. These devices are subject to the same policies and, technical controls as all other devices which are considered static.

11.2 Tablets and smart phones

11.2.1 These types of devices are not exempt from the controls mentioned in this policy or other related SOPs. They should be managed in line with desktop and laptop assets.

12.0 PHYSICAL AND ENVIRONMENTAL SECURITY

12.0.1 Physical and environmental security is an important aspect of protecting the Trusts network, systems and data. All equipment should be protected against loss or damage or outside unauthorised interference to protect against interruption to frontline services or business activity.

12.1 Purchase of Equipment (Supply Chain)

12.1.1 All purchases of new systems hardware or new components for existing systems must be made in accordance with Information Security and other Organisation Policies, as well as technical standards.

12.1.2 Except for minor purchases, hardware must be purchased through a structured evaluation process which must include the development of a detailed request for proposal document. Information Security features and requirements must be identified with the document.

12.1.3 All new hardware installations are to be planned formally and notified to all interested parties ahead of the proposed installation date. Information Security requirements for new installations are to be circulated for comment to the Information Governance Team, well in advance of installation.

12.2 Maintenance

12.2.1 Network, and infrastructure equipment is generally managed by the Trusts in-house IT Teams, and therefore they are ultimately responsible for the maintenance of the Trusts equipment

12.2.2 All central processing equipment, including file servers, will be covered by third party maintenance agreements.

12.2.3 All computers, terminals and printers will be covered by maintenance agreements (where such provision is not in-house) with third parties for repair of out of warranty equipment provided it is cost effective (each case will be judged on its merits).

12.2.4 All such third parties will be required to sign a Confidentiality Code of Conduct.

12.3 Equipment Siting and Protection

12.3.1 Information Management/Technology Systems equipment should always be installed and sited in accordance with the manufacturer’s specification.

12.3.2 Equipment should be sited to reduce risks from environmental threats, and from unauthorised access. Where equipment must be kept in public areas, it should be positioned to reduce the risk of unauthorised access or casual viewing.

12.3.3 Environmental controls will be installed to protect central/key equipment. Such controls will trigger alarms if environmental problems occur. In such cases only authorised entry will be permitted.

12.3.4 Smoking, drinking, eating and the use of mobile phones or other radio-frequency devices is not allowed in areas housing key computer and network equipment and doors should be kept locked at all times. Warning signs to this effect must be prominently displayed at the entrance.

12.3.5 Appropriate measures must be taken to minimise the risk of theft of computing equipment. Consideration shall be given to measures such as secure anchoring of such equipment in public places and security coding/marking.

12.3.6 All devices, which include Desktops computers, Laptops, mobile devices, USB removable drives will be encrypted by default.

12.3.7 Any room which contains any IT Infrastructure equipment is to be used for that purpose only. These rooms (known as “comms rooms”) are not to be used for any other purpose. The storage of any items not vital to the functioning of the IT Infrastructure equipment is strictly forbidden. This includes boxes or bags of rubbish, cleaning equipment/supplies, Office supplies, or broken/old IT equipment.

12.4 Power Supplies

12.4.1 All critical computer equipment will be fitted with battery back-up, using uninterruptible power supplies (UPS), to ensure it does not fail during switchovers between mains and generator (where available). These UPS units must provide sufficient power to ensure the relevant system(s) can be shut down gracefully in the event of supply restoration/generator back-up not being available. Where a system is not manned continually, management software should be installed to allow the automatic shutdown of the system in the event of a power failure.

12.4.2 Critical computer sites will be fitted with emergency power off switches for use in a crisis. Such sites will have their own mains circuits not subject to power surges from other parts of the building or locality.

12.5 Location Controls

12.5.1 All central processors/networked file servers/central network equipment should always be located in secure areas with restricted access.

12.5.2 The Trust’s central computer site will be in high security area housing with entry restriction and a detection system will be incorporated to protect the site.

12.5.3 Local network equipment/file servers and HSCN Network terminating equipment will always be located in secure areas and/or lockable cabinets.

a) All network computer equipment will be housed in a controlled and secure environment.
b) All cabling (electricity and communications) between and within buildings need to be inaccessible to unauthorised people
c) All designs applied and materials used must comply with relevant standards in relation to data, cabling, electrical and heating services.
d) Critical or sensitive network equipment:
    I. Will be housed in secure areas, protected by a secure perimeter, with appropriate security barriers and entry controls.
    II. Will be protected from power supply failures.
    III. Will be protected by intruder alarms and fire suppression systems.
    IV. Where room gas fire suppression is present, warning notices must be issued with any instructions for room evacuation.

12.6 Access Control to Secure Network Areas

12.6.1 Entry to secure areas housing critical or sensitive network equipment will be restricted to those whose job requires it. Trust's network team(or other such provider) will maintain and periodically review a list of those with unsupervised access.

12.7 Secure Disposal or Re-use of Equipment

12.7.1 Computer hardware disposal can only be authorised by the Director of Finance as laid out in the Trust' Standing Financial Instructions. All data storage devices on hardware that are to be disposed of will be purged of confidential data before disposal or securely destroyed. The procedures for disposal will be documented.

12.7.2 The Assistant Director of IT will be responsible for ensuring that correct vetting procedure is followed while selecting the disposal company and a contract is drawn up between the Trust and the Third party to ensure that the following is adhered to:

a) Disposal company is a fully accredited ISO: 27001 IT waste disposal organisation.
b) All required standards for the destruction of Health Care Data are met.
c) Disposal company has an auditable process for asset tracking and data destruction.
d) A full disposal inventory is held with relevant data destruction certificates by the Trust IT team.
e) Have professional indemnity insurance.

12.7.3 The IT Service Manager, IT Infrastructure Manager, and Cyber Security Specialist will ensure adherence to this process.

12.7.4 When an item of IT equipment or media is no longer required contact the IT Service Centre on 0300 123 1885 and you will be asked to complete a service request form which is located on the IT Service Centre portal.

12.7.5 Disposal and the associated procedures are managed by the IT Service Centre, who are also responsible for maintaining an inventory of items disposed of.

12.7.6 Under no circumstances should an individual dispose any IT equipment or media independently of the contract or IT service.

12.7.7 Do not release IT Equipment or media until you have been authorised to do so and only to IT personnel. Always ask to see ID.

12.7.8 IT Equipment and Media includes, but is not limited to:

- USB drives
- Any removable media device
- Computers
- Laptops
- Tablets
- Scanners
- Printers
- Photocopiers
- Scanners
- MFDs
- Mobile phones
- Cameras / recording equipment (which contain data on memory)
- Fax machines (although use of these is strictly prohibited now)

12.7.9 KCHFT has a responsibility to destroy all electronic waste in accordance with the Waste Electrical and Electronic Equipment (WEEE) Directive and other environmental standards.

12.7.10 There are safeguards in place to protect the asset and the information contained within it and auditable trails for disposal and destruction which must be documented by the IT Service Centre.

12.7.11 The Trust will, if deemed necessary, visit the Supplier's data destruction depot and waste disposal depot to assure that disposals adhere to NHS standards for disposing of assets from the point they are collected through to the end of the process.

12.7.12 For Full process see; SOP - IT Disposal Process

12.8 Temporary Local Storage of End-of-Life assets

12.8.1 Assets for disposal are collected from users on request and moved by a member of the IT department, and transported to secure temporary stores. At present these stores are sited at

a) Shearway, Folkestone
b) Trinity House, Ashford
c) St Augustine's College in Westgate
d) Gravesham Community Hospital
e) Snodland Clinic

12.8.2 Access to the rooms is limited to the necessary IT personnel and must be secured at all times.

12.9 Security of Physical Media in Transit

12.9.1 Where physical media needs to be sent via postage methods reliable transport or couriers should be used, and a procedure to check the identity of couriers in the event of loss or damage of media or equipment should be implemented.

12.9.2 Packaging should be sufficient to protect the contents from any physical damage likely to arise, in accordance with the manufacturer's specifications. Regard should be given to any adverse environmental conditions that may occur during transit.

12.9.3 Special controls should be adopted, where necessary, to protect confidential information and organisational assets from unauthorised disclosure or modification, such as;

a) Use of secure Containers
b) Delivery by Hand
c) Tamper-evident packaging
d) Tracer Card

12.9.4 All non NHS agencies/organisations will be required to sign security and confidentiality agreements with the Trust when transferring data. If necessary, a Data Protection Impact Assessment should be completed prior to transferring personally identifiable information.

12.9.5 Bulk transfers of data from one medium to another (CD – PC – Memory Stick or Location to Location) should be arranged with the IT Team by logging a call with the IT Service Centre.

12.10 Lost or Stolen

12.10.1 Please refer to the Data security and protection policy for information on what to do in the case of lost or stolen equipment.

13.0 DATA

13.1 Unauthorised data removal or theft

13.1.1 Under no circumstances should information containing patient or Trust information be removed from the Trust's network for personal use or personal/economic gain.

13.3 Information Classification

13.3.1 KCHFT will ensure all data held on the systems identified on the asset inventory can be classified as either patient or non-patient information.

13.3.2 The Trust must record, maintain and update a register of its information assets.

13.3.3 All information, data and documents must be processed and stored strictly in accordance with the classification levels assigned to that information.

13.3.4 All information, data or documents classified as highly sensitive must be stored in a separate secure area.

13.3.5 All information, data and documents must be classified according to their level of confidentiality, sensitivity, value and criticality.

13.3.6 All information, data and documents are to be the responsibility of a designated information owner or custodian.

13.3.7 Access to the resources available from The Trust' network must be strictly controlled in accordance with the agreed Access Control List, which must be maintained and updated regularly.

13.6 Protecting Data in Transit

13.6.1 All network traffic over the VPN will be encrypted to the required standards, and require two factor authentication.

13.6.2 External Access to all the Trusts intranet sites will be over HTTPS, using the required TLS protocols.

13.6.3 All emails containing Patient data or PII will be sent from and to an email address which supports the required level of encryption, or using the [secure] tag

13.6.4 Large files containing sensitive or private data which cannot be sent by email must still be sent encrypted and password protected using an appropriate system which has been through the KCHFT DPIA process.

13.6.5 Use of Dropbox, One Drive and similar are not a permitted method of storing or exchanging PII, Patient Data or any information of a sensitive nature which relates to the Trust.

13.6.6 Exchange of files containing PII or sensitive information must be done using a trust approved system. These systems will be listed on flo.

13.7 Protecting Data at Rest

13.7.1 All remote equipment, including Laptops, and tablets will have its internal storage encrypted to the required standards and be centrally managed by responsible IT Team.

13.7.2 The Trust will limit the amount of data stored locally, ensuring that sensitive information is stored centrally on the Trusts network and not on the device where possible.

14.0 AVAILABILITY MANAGEMENT

14.0.1 Availability of information systems, services and associated processes is critical to our clinical and business operations. System availability consideration shall therefore be assessed and documented and considered when architecting and implementing new systems and services.

14.0.2 Information system availability requirements shall be established and documented in conjunction with systems owners and appropriate stakeholders and shall include maximum time to restore information systems and services (in days / hours). Availability requirements and targets shall be included in business continuity planning activities and shall be reviewed at least annually.

14.0.2 Availability requirements for new information systems and services shall be identified and documented during the system design stage and shall be built in to systems architecture during implementation.

14.0.3 System acceptance testing shall be carried out to ensure the documented availability requirements have been met before system go-live.

15.0 TRAINING AND AWARENESS

15.0.1 KCHFT has developed an induction programme to ensure that all staff, undertake Information Governance training at the start of their employment with the Trust in accordance with the Data Security and Protection Toolkit.

16.0.2 In addition to the induction programme, there is a web-based e-tutorial programme covering all elements of the Data Security and Protection Toolkit which all staff will be required to complete. As part of this programme, all staff will be made aware of their responsibilities and the possible actions with regard to breaches of information security e.g. reporting procedures, identifying further training and possible disciplinary action. This training will be audited externally to provide assurance of its compliance and suitability.

15.0.3 Information Governance issues and training should be included within the Continuing Development Plans (CDP) for all staff as part of their annual staff assessments and recorded in their Professional Development Plans (PDP).

16.0 MONITORING COMPLIANCE AND EFFECTIVENESS OF THIS POLICY

16.0.1 Managers are responsible for performance monitoring their teams with regard to training and this should be built into staff appraisals.

16.0.2 The Information Governance Assurance Group will be responsible for leading on the implementation of this policy and other Information Security related policies and procedures. It will ensure that clear formal guidelines have been provided to staff on all aspects of Information Security.

16.0.3 The review or creation of other Information Security related policies and procedures will include mechanisms for monitoring compliance with this policy or other procedural standards.

16.0.4 This policy and related procedures will be continually monitored and will be subject to regular review, which will take place annually from the date of issue. The Information Governance Assurance Group will carry out the review.

16.0.5 An earlier review may be warranted if one or more of the following occurs:

a) as a result of regulatory / statutory changes or developments
b) as a result of NHS policy changes or developments
c) for any other relevant or compelling reason

16.0.6 KCHFT will establish appropriate confidentiality audit procedures in line with the requirements of NHS Digital.

16.0.7 KCHFT will work closely with the Audit Committee to assist in conducting audits across KCHFT, in areas where low scores have been recorded following the Information Security baseline assessment

16.0.8 Monitoring matrix:

What will be monitored?	**How will it be monitored?**	**Who will monitor?**	**Frequency**
Audit of impact and compliance	Number of incidents clinical or non-clinical)	Information Governance Assurance Group	Bi-monthly
Staff training	Through annual IG training	Information Governance Assurance Group	Bi-monthly
Staff awareness of the documents and associated requirements	Through annual IG training and line management process	Line managers to ensure mandatory training is updated and policy signature sheet is complete	Annually

17.0 EXCEPTIONS

17.0.1 Any exceptions are noted in the policy above, and there are no additions to this..

18.0 GLOSSARY AND ABBREVIATIONS

Access Control The prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner

Accountability The property that will enable the originator of any action to be identified (whether the originator is a human being or a system)

Application Manager Nominated person responsible for the operational management and development of software for a specific system

Asset Owner Individual or organisation having responsibility for specified information asset(s) and for the maintenance of appropriate security measures

Audit Trail Data collected and potentially used to facilitate any reconstruction of events within the system

Authentication Corroboration of the origin and correctness of any part of the system

Authorisation The granting of rights, which includes the granting of access based on access rights

Availability Information is delivered to the right person, when it is needed

BCDRP The Trusts Business Continuity and Disaster Recovery Plan

Brute Force Attacks	A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data.
Confidential	Confidential information includes, but is not limited to, all information of a confidential nature relating to the business and affairs of The organisation, its' patients and employees, and any business or affairs of any other person to whom The organisation has an obligation of confidentiality.
CareCert	CareCert is NHS Digital's Care Computer Emergency Response Team. This is a cyber security centre of excellence and provides warnings, advice and guidance for all NHS and Social Care organisations
Chain of Custody	The chronological documentation or paper trail that records the sequence of **custody**, control, transfer, analysis, and disposition of physical or electronic evidence.
Criminal Hackers/ Saboteurs	The probability of this type of attack is low, but not entirely unlikely given the amount of sensitive information contained in NHS databases. These attackers are likely to be trained in the use of the latest hacking tools. Attacks are well planned and based on weaknesses discovered that will allow a foothold into the network.
CIRP	The Trusts Cyber Incident Response Plan
CNIS	The Trusts Cyber Network and Information Security Policy
Datix	The Trusts online incident reporting tool
Data Controller	Data controller means a person who (alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed and the data are in the form in which they have been or are intended to be processed or recorded with that intention or as part of a relevant filing system or is part of an accessible record and processing means obtaining, recording or holding the information or data, including organisation, retrieval, disclosure, blocking, erasure or destruction. [Data Protection Act (1998)]
Denial of Service (DoS/DDoS)	The prevention of authorised access to resources or the delaying of time critical operations. If multiple sources are used it becomes a Distributed Denial of Service.
DPIA	Data Protection Impact Assessment
DSPP	Data Security and Protection Policy
Hackers	Sometime known as vandals are people who are the most common type of attackers on the Internet. The probability of attack is extremely high they scan the internet looking for well-known software security holes.

	Web servers and electronic mail are favourite targets. They exploit weaknesses to plant viruses, or use the resources of your system for their own means. If they do not find an obvious weakness they are likely to move on to an easier target.
Health Record	This is any record which consists of information relating to the physical or mental health or condition of an individual made by or on behalf of a health professional in connection with the care of that individual
Impact	The embarrassment, harm, financial loss, legal or other damage which could occur in consequence of a particular security breach
IM	Information Management
IT	Information Technology
Integrity	All system assets are operating correctly according to specification and in the way that the current user believes them to be operating
Lateral Movement	When a malicious attacker who has compromised a machine on the network then uses other exploits to move around the network to different machines/PCs.
Malware	A term used to refer to various forms of intrusive or hostile computer software, such as viruses, worms and Trojan horses
NIS	Network and Information Security Directive. Lawfully enforceable directive for essential public services.
NHS Organisations	All organisations providing health care services, including health authorities, special health authorities, trusts, general medical and dental practices
Password	Confidential authentication information composed of a string of characters
Phishing	The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online.
Personally Identifiable Information (PII)	Data consisting of data which relate to a living individual who can be identified from that data (or from that and other information in the possession of, or likely to come in the possession of, the Data Controller), including any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual *[Data Protection Act (2018)]*
Privilege Creep	Used to describe when over time a user “gathers” advanced privileges and ends up with privileges way above what they need. Normally occurs with long serving members of staff.
Special	Any feature or facility of a multi-user system that enables a user to

Privilege	override system or application controls
Risk	The likelihood of occurrence of a particular threat, with the degree of vulnerability to that threat and the potential consequence of the impact if the threat occurs
Risk Assessment	Comprehensive concept for defining and assessing the potential impact of threats to, and vulnerabilities of, computer system assets and capabilities, and for supplying management with information Suitable for a (risk management) decision in order to optimise investment in security counter-measures
Security Audit	A review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policies and operational procedures, to detect security breaches and to recommend any indicated changes in control policy and procedures
Security Breach	Any event that has, or could have, resulted in loss or damage to NHS assets, or an action that is in breach of NHS security procedures
Smart Card	A physical security token used in conjunction with a password to provide a higher level of protection for authentication.
Security Policy	A statement of the set of rules, measures and procedures that determine the physical, procedural and logical security controls imposed on the management, distribution and protection of assets
Sensitive Personal Data	This is data as to the Data Subject's: a) Racial or ethnic origin b) Political opinions or religious beliefs c) Trade union membership d) Physical or mental health or condition e) Sexual life f) Criminal offences, proceedings or convictions *[Data Protection Act (1998)]*
Sensitivity	A measure of importance assigned to information to denote its confidentiality
Spam	Irrelevant or unsolicited messages sent over the Internet, typically to large numbers of users, for the purposes of advertising, phishing, spreading malware, etc.
Spoofing	The creation of email messages with a forged sender address. A forged sender address uses a respected or reputable origin email address to conceal the fact that the email has come from elsewhere.
System Manager	Nominated IM/IT person responsible for the hardware and operating system and database management for a specific system

Threat	An action or event that might prejudice security
VPN	Virtual Private Network. (An encrypted tunnel to the internal network)
Vulnerability	A Security weakness in Software Design, configuration, lack of Controls in place, or the action/potential action of an individual using the Network
PID/PII	Personally identifiable information (PII) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.
2FA	2 Factor Authentication. (The use of a second form of authentication. Password and Smart Card for example)
APT	Advanced Persistent Threat. Highly organised, possibly State Funded, well-resourced groups who present a constant, high level, sophisticated threat to the organisation.