NHS
Kent Community Health
NHS Foundation Trust

Data Security and Protection Policy

Document Reference No.	KIG025
Status	FINAL
Version Number	1.9
Replacing/Superseded policy or documents	1.8
Number of Pages	51
Target audience/applicable to	All individuals carrying out work on behalf of Kent Community Health NHS Foundation Trust
Author	Information Governance Team
Contact Point for Queries	Information Governance Team
Date Ratified	4 May 2023 (CARM)
Date of Implementation/distribution	4 May 2023
Circulation	Policy dissemination process and on-line
Review date	February 2025
Copyright	Kent Community Health NHS Foundation Trust

EXECUTIVE SUMMARY

Scope and purpose of Policy

This policy provides a summary/overview of how an organisation is addressing the Information Governance (IG) agenda.

This policy is a culmination of the IG policies, shown on page 4 which includes the Information Governance Management Framework (IGMF). All procedures and supporting policies mentioned in this policy are available on Flo.

This policy has been aligned with UK GDPR requirements and the Data Security and Protection Toolkit.

It covers the policy statement in regard to:

- Data protection and confidentiality
- Processing of personal confidential data
- Record management
- Roles, responsibilities and accountabilities
- Governing bodies and legal obligations
- Training
- Incident management
- Risk management
- IT protection (Cyber and Network Information Systems Policy)
- Monitoring, auditing and reporting

This policy applies to all staff whether permanent, temporary, locum, bank, volunteers or contractors employed directly or any individual working on behalf of Kent Community Health NHS Foundation Trust (KCHFT).

Implementation of this policy will contribute significantly towards assuring KCHFT patients and staff that their information will be processed in compliance with legislative, ethical and national NHS policy requirements.

Each section of the policy provides more detail on the way in which the different initiatives are managed and encompass all information used by KCHFT including the use of information systems.

Any member of staff in breach of IG requirements contained within this policy or supporting policies may be subject to disciplinary action according to KCHFT disciplinary policy, up to and including dismissal if deemed appropriate.

For further guidance refer to the HR Disciplinary Procedure on Flo.

Risks addressed

It is important all staff be made aware through documentation and training and awareness sessions that they must meet IG requirements and it is made clear to them that breaching these requirements e.g. patient confidentiality is a serious disciplinary offence.

Governance Arrangements

Governance Group responsible for developing document	Information Governance Assurance Group (IGAG)
Circulation group	IGAG, Corporate Assurance and Risk Management Group, Executive Team and all staff through Flo
Authorised/Ratified by Governance Group/Board Committee	CARM
Authorised/Ratified On	4 May 2023
Review Date	February 2025
Review criteria	This document will be reviewed prior to review date if a legislative change or other event dictates.

Key References

A guide to confidentiality in health and social care: references: Treating confidential information with respect
Access to Health Records Act 1990
APCO Good Practice Guide for Computer based Electronic Evidence V3
BS ISO / IEC 27001: 2005 Information Security Management
BS ISO / IEC 17799: 2005
Care Quality Commission Standards
Common Law Duty of Confidentiality
Computer Misuse Act 1990
Copyright, Designs and Patents Act 1988
Criminal Investigation and Procedures Act 1996
Data Protection Act 1998/2018 (Data Protection Bill)
Department of Health Caldicott Manual: NHS Code of Practice
Department of Health Confidentiality: NHS Code of Practice 2003
Department of Health Information Security Management: NHS Code of Practice 2007
Records Management Code of Practice 2021
Digital Preservation Coalition: Digital Preservation Handbook: https://www.dpconline.org/handbook
Freedom of Information Act 2000
Good Practice Guide for Computer-based Electronic Evidence
Health and Social Care Act 2012
NHS Digital NHS Information Risk Management Digital Information Policy (2009)
NHS Digital Data Security and Protection Toolkit
NHS Digital Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation (Feb 2015)
NHS Digital Guide to Confidentiality in Health and Social Care (Sept 13)
Human Rights Act 1998
ICO website www.ico.gov.uk for codes of practice
Information: To Share Or Not To Share? The Information Governance Review 2013
Kent Police and Kent Health Sector Bodies: Joint Working Agreement
NHS Care Record Guarantee 2011
NHS Constitution 2013
NHS Information Governance: Guidance on Legal and Professional Obligations (DH 2007)
NHS: Personalised Health and Care 2020 – Using data and technology to transform outcomes for patients and citizens (Nov 14)

Police, Criminal Evidence and Terrorism Act (PACE)
Public Records Act 1958
Regulation of Investigatory Powers Act 2000
Report on the Review of Patient Identifiable Information (Caldicott Committee 1997)
Care Quality Commission Safe data, safe care report (2016)
National Data Guardian for Health and Care review of Data Security, consent and opt-outs (2016)
Department of Health Protecting Healthcare Information (2014)
Department of Health Your Data: Better Security, Better Choice, Better Care (2017)
The Data Protection Processing of Personal Data Order 2000
The Public Interest Disclosure Act 1998
EL(92)60 Code of Practice for the Secure Handling of Confidential Information
BS7799 British Standard of Information Security Systems
NHS England Accessible Information Standard
UK General Data Protection Regulations (UK GDPR)
Department of Health and Social Care: Prevent and the Channel process in the NHS: information sharing and governance

Related Policies/Procedures (all available on Flo)

Title	Reference
Cyber, Network and Information Systems Policy	KIG026
Being Open Policy (incorporating Duty of Candour)	IML004
Confidentiality Code of Conduct	KCRM005
Data Quality Policy	RM008
Freedom of Information Act 2000 Policy (including EIRs and RPSI)	KIG017
Incident Policy	CQS016
Serious Incident Policy	CQS027
Home, Remote and Mobile working Standard Operating Procedure	KIG034
Registration Authority Policy	RAM001
Secondary Use of Personal Data Policy	KIG021
Transfer of Care Policy	QC003
Deteriorating Patient Standard Operating Procedure	QC004
Safe haven guidance	On Flo
How to appraise, retain and dispose of records	On Flo
How to keep a Clear Screen and Clear Desk	On Flo
How to archive – flowcharts	On Flo
How to email and text patients	On Flo
How to ensure the security and confidentiality of records	On Flo
How to scan records	On Flo
How to lock print (not Papercut)	On Flo
How to print from home	On Flo
How to keep a clinical diary and printed caseload tool	On Flo
How to obtain an NHS number	On Flo
How to send confidential information by post	On Flo
How to share information with the Police	On Flo
How to share information – Caldicott Principles	On Flo
How to transport paper clinical and staff records	On Flo
How to define the legal basis for processing patient information	On Flo

Risk assessment for transportation and storage of personal confidential or business sensitive information off-site	On Flo
Maintaining personnel files guidance	On Flo

Document Tracking Sheet

Version	Status	Date	Issued to/approved by	Comments / summary of changes
0.1	First draft	Jan 2018	N/A	
0.2	Second draft	May 2018	For general consultation	Updates to sections in line with GDPR and IG Alliance Guidance
0.3	Third draft	May 2018	IGAG	Approved, subject to feedback from consultation phase
0.4	Final draft	May 2018	CARM	For virtual ratification, subject to feedback from consultation phase.
1.0	FINAL	May 2018	N/A	Formatting and numbering tidied prior to publication.
1.1	FINAL	June 2018	IG Compliance Manager	Minor amendment to section 22.5
1.2	FINAL	Jan 2019	IG Compliance Manager/ IG Assurance Lead	Minor amendment to paragraphs 3.3.6, 22.5.7, minor grammar and formatting amendments through, related policies and procedures updated
1.3	FINAL	May 2019	IG Compliance Manager	Minor amendments removing IG generic email addresses
1.4	FINAL	July 2019	IG Assurance Lead	Minor correction to protected characteristics on page 11 – 'age' moved to a separate bullet point on its own
1.5	FINAL	Sept 2019	IG Compliance Manager/IGAG	Minor amendments: • Key references & grammar updated • IG audits now renamed as IG Service Reviews • Privacy Impact Assessments renamed as Data Protection Impact Assessments • Disposal of clinical records on site in confidential waste • Extra clarity added to section 25 around records management/preservation of electronic systems, scanning of records & regular destructions
1.6	FINAL	Jan 2021	IG Compliance Officer	Minor amendments • 8th Caldicott Principle added. • All Flo links updated and links checked throughout document.

1.7	Final	Dec 21	IG Compliance Officer/IG Assurance Lead	• Updated key references • Updated related policies and procedures • Updated various paragraphs in section 25 to highlight the requirement to hold some records for extended retention periods and provide other clarification points (25.1, 25.9 and 25.20) • GDPR references changed to UK GDPR • Audio Visual Recording Added
1.8	Final	March 2022	IG Compliance Officer	• Update to job role of Caldicott Guardian.
1.9	FINAL	4 May 2023	CARM	• DHSC's "Prevent and Channel process in the NHS for information sharing and governance" added to key references section • 3.9 Caldicott Principles wording updated • 9.0 key senior roles updated • Job titles updated • 21.3 MS Teams and other mobile communications added as record types • Removal of corporate services references • 22.0 RM strategy updated • 22.20 inclusion of content lists retention period • 27.0 contact details updated • Minor grammar and formatting changes • Reference to IG newsletter frequency removed

EQUALITY ANALYSIS

Has an Equality Analysis (EA) been completed?
No ☐ The document will have no impact on people with any of the nine protected characteristics
Yes ☐ *Include summary of any reasonable adjustments or actions required to avoid significant impact on patients, patients' families and employees and volunteers with protected characteristics.* The Equality Analysis for this policy is available upon request by contacting the Engagement Team via kchft.equality@nhs.net.
NOTE: *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.* *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.* ***Protected characteristics:*** *Age, Disability, Gender Reassignment, Marriage and Civil Partnership, Pregnancy and Maternity, Race, Religion and Belief, Sex, Sexual Orientation.* *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.* ***Equality Analysis*** *Liaise with the Engagement Team if support is required at kchft.equality@nhs.net*

CONTENTS

Further information on this policy and other Information Governance matters can be found on Flo.

FOREWORD

Information Governance (IG) allows Kent Community Health NHS Foundation Trust (KCHFT) and all individuals to ensure personal confidential data is handled legally, securely, efficiently and effectively, in order to deliver the best possible care for its patients.

Additionally, IG enables KCHFT to put in place procedures and processes for their corporate information that support the efficient location and retrieval of corporate records, where and when needed, to meet requests for information and assist compliance with corporate governance standards.

IG is a business-wide support service necessary to ensure key messages and behaviours are communicated throughout the organisation. The work of the IG team is supported by the Data Protection Officer (DPO), Senior Information Risk Owner (SIRO) and the Caldicott Guardian (CG).

KCHFT is committed to ensuring all individuals undertaking work on behalf of the trust, are aware of their personal responsibilities, and are equipped with the skills required to dispense advice and communicate with patients, public, other organisations and their colleagues effectively.

It is important all staff be made aware, through documentation, training and awareness sessions, that they must meet IG requirements and it is made clear to them that breaching these requirements e.g. patient confidentiality; is a serious disciplinary offence that could lead to dismissal.

There is a formal disciplinary process in place and documented procedures are available from the Human Resources department. IG breaches are clearly referenced and all those undertaking work on behalf of the organisation should familiarise themselves with the consequences of misconduct.

This policy's objective is to help KCHFT and individuals to be consistent in the way they handle personal confidential data 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.

It is important that this policy is not read in isolation but read alongside the supporting policies available.

For further information and to view the supporting policies and training opportunities visit the IG page on Flo. All staff are also encouraged to sign up to the IG Workspace on Flo.

....	....	....
Senior Information Risk Owner (SIRO)	Caldicott Guardian (CG)	Data Protection Officer (DPO)

1.0 WHAT IS INFORMATION GOVERNANCE?

1.1. Information Governance (IG) is the way organisations process or handle information. It covers personal information, relating to patients, service users and employees and corporate information such as financial and accounting records.

1.2 IG provides a framework to bring together all the rules, whether legal or simply best practice, that apply to the handling of information, supporting:

- high quality care
- compliance with the law
- implementation of central advice and guidance, and
- year or year improvement

1.3 At its heart, IG is about identifying a high standard for the handling of information and giving the organisation and its employees the tools to achieve that standard.

1.4 IG provides a consistent way for the trust and its employees to deal with the many different standards and legal rules that apply to information handling, including:

- data protection and confidentiality
- information sharing for care and non-care purposes
- information security and information risk management
- information quality
- records management for both care and corporate information.

2.0 THE DATA SECURITY AND PROTECTION POLICY

2.1 This policy outlines robust, clear and effective IG accountability structures, governance process and procedures in line with legislation and best practice.

2.2 Scope of the policy

2.2.1 This policy will identify key roles and organisational, management and staff accountability and responsibilities. It will provide the necessary guidance to maintain compliance with the law and best practice for all employees of the trust.

2.2.2 This policy does not differentiate between types of record, media or subject. It is based on current legislation and will be updated to reflect changes as they occur therefore the electronic version of this document on Flo will be the most current.

2.2.3 Do not print this document as there may be more up to date versions on Flo.

2.2.4 This policy applies to all individuals whether permanent, temporary, locum, bank or contractors that are employed directly or working on behalf of KCHFT. Individuals for the purpose of this policy will be referred to as “staff”.

2.2.5 There are additional supporting policies which may be relevant. These will be signposted within the policy as necessary. This policy must not be read in isolation of the documents mentioned.

2.3 The law and best practice

2.3.1 This policy is based entirely on legislation and NHS best practice and its content is mandated to all employees. By signing your employment contract or volunteer agreement, supported by the Confidentiality Code of Conduct you agree to work within the principles stated and current data protection law.

2.3.2 A duty of confidence arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence.

- it is a legal obligation that is derived from case law;
- it is a requirement established within professional codes of conduct; and
- is included with your employment contract as a specific requirement linked to disciplinary procedures.

2.3.3 Patients and employees allow the trust to gather sensitive information relating to their health, employment. They do so in confidence and they have the legitimate expectation that staff will respect their privacy and act appropriately.

2.3.4 In some circumstances patients may lack the competence to extend this trust, or may be unconscious, but this does not diminish the duty of confidence.

2.3.5 The trust is committed to the delivery of a first-class confidential service. This means ensuring all personal information is processed fairly, lawfully and as transparently as possible so that is understood why;

- their personal data is being processed
- give their consent for the disclosure and use of their personal information
- gain trust in the way the NHS handles information and;
- understands their rights to access information held about them

2.3.6 The trust must publish why the information given may be recorded and shared and the legal basis for doing so.
For staff there is a privacy notice on Flo and available on “My ESR”.
For patients the Privacy Notice and patient leaflet ‘What happens to personal information held about you?’ must be clear and concise and provide all the information stipulated in law. The notice is available in printable format on Flo and in electronic format on the trust’s website.

3.0 THE DATA PROTECTION ACT

3.1 The current Data Protection Act governs the use and protection personal data (information) relating to a living individual. The Act does not apply to personal data relating to the deceased.

3.2 For any organisation processing (obtaining, holding, using, disclosing and disposing etc.) data, it is the “Data Controller’s” (KCHFT) responsibility for abiding by the six data protection principles and notifying the Information Commissioner of that processing.

3.3 Any high-risk processing of individuals data must be reported to the Information Commissioner’s Office who are the UK’s independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. For further information see https://ico.org.uk

3.4 The Act gives eight rights to individuals in respect of their own personal data

3.5 Both the principles and rights of the individuals within the Act are explained in detail below. Rights of access to information are covered in the Access to Records Policy and the patient leaflet "What happens to personal information held about you?"

3.6 Data Protection Principles

3.6.1 The following six principles are an extract from the Data Protection Act 2018. The principles are law and based on the rights of the data subjects, as listed below. They must be complied with, at all times.

Principle	Description
1	Processing of personal data must be lawful, fair and transparent
2	The purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and must not be processed in a manner that is incompatible with the purpose for which it is collected
3	Personal data must be adequate, relevant and not excessive in relation to the purpose for which it is processed.
4	Personal data undergoing processing must be accurate and, where necessary, kept up to date.
5	Personal data must be kept for no longer than is necessary for the purpose for which it is processed.
6	Personal data must be processed in a manner that includes taking appropriate security measures as regards risks that arise from processing personal data. This includes, but is not limited to, accidental or unauthorised access to, or destruction, loss, use, modification or disclosure of personal data

3.7 Accountability principle

3.7.1 In addition to the principles above cited in Article 5 (1) there is a further principle in Article 5 (2) of the UK GDPR concerning `accountability` whereby organisations must be able to demonstrate compliance. This accountability is reinforced by the specific responsibilities of KCHFT as a data controller under Article 24, to implement appropriate technical and organisational measures, including policies where proportionate in relation to processing activities.

3.7.2 The focus for the accountability principle is evidence-based compliance with specified requirements for transparency, more extensive rights for data subjects and considerably harsher penalties available for non-compliance.

3.7.3 The Key obligations supporting accountability KCHFT must meet are:

- appointment of a Data Protection Officer.

- the recording of all data processing activities with their legal basis and data retention periods
- ensuring that DPO is involved at an early stage in all data protection matters, assesses the need for data protection impact assessment and monitors their effectiveness
- in particular conducting a data protection impact assessment where processing health data on a large scale
- implementing measures such as data minimisation, pseudonymisation etc.
- ensuring demonstrable compliance with enhanced requirements for transparency and fair processing, including notification of rights
- ensuring data subject rights are respected
- notification of personal data breaches and communicating breaches to the data subjects where it is likely to result in high risk to their rights and freedoms
- having technical and organisational measures in place that ensure and demonstrate KCHFT comply, for example policies, procedures, provision and monitoring of training.

3.8 Rights under the Act

3.8.1 All individuals, or subjects as they are known in law, have rights within the law. Every employee has a responsibility to ensure these rights, where applicable, are upheld. If you have any queries, please contact the Trust's Data Protection Officer

Right	Description
1. The right to be informed	This allows individuals to know who is holding their data, why it is being processed and other specific information that must be supplied (this is also found on the KCHFT privacy poster and patient leaflet "What happens to personal information held about you?"
2. The right of subject access	This allows individuals to find out what information is held about them (see the Access to Health Records Policy on Flo)
3. The right to rectification, blocking, erasure and destruction	Individuals are entitled to have personal data rectified if it is inaccurate or incomplete
4. The right to erasure	Individuals can apply their "right to be forgotten" in some circumstances. If staff wish to exercise this right please speak to HR in the first instance. In the healthcare context the right to be forgotten does not apply – this is for information only.
5. The right to restrict processing	Individuals have the right to 'block' or suppress processing of personal data under certain conditions.
6. The right to data portability	Individuals have the right to receive personal data about them in a 'commonly used and machine-readable format'. This right is only available where the processing is based on consent and the processing is automated.

7. Rights in relation to automated decision taking (including profiling)	Individuals have a right to object to decisions made only by automatic means e.g. there is no human involvement
8. The right to object	Individuals have the right to object to: •processing based on the performance of a task in the public interest/exercise of official authority (including profiling); •direct marketing (including profiling); and •processing for purposes of scientific/historical research and statistics (although certain conditions apply)

3.9 Caldicott Principles

3.9.1 The eight Caldicott Principles were devised by the Caldicott Committee. They represent best practice for using and sharing identifiable patient information. However, the same should be applied whenever a disclosure of personal information is being considered.

Principle	Description
1	Justify the purpose(s) for using confidential information
2	Use confidential information only when it is necessary
3	Use the minimum necessary confidential information
4	Access to confidential information should be on a strict need to know basis
5	Everyone with access to confidential information should be aware of their responsibilities
6	Comply with the law
7	The duty to share information for individual care is as important as the duty to protect patient confidentiality
8	Inform patients and service users about how their confidential information is used.

3.10 Data Security Principles

3.10.1 The following ten Data Security Principles were published by the National Data Guardian in 2017. The principles provide the foundation to the annual self-assessment the trust has to complete annually. These are also published in more detail in the Cyber and Network Information Systems policy.

Standard	Description

1	All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is shared for only lawful and appropriate purposes.
2	All staff understand their responsibilities under the National Data Guardians data security standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
3	All staff complete appropriate annual data security training and pass a mandatory test, provided through the redesigned Data Security and Protection Toolkit.
4	Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All instances of access to personal confidential data on IT systems can be attributed to individuals.
5	Processes are reviewed at least annually to identify and improve any which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
6	Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken as soon as possible following a data breach or near- miss, with a report made to senior management within 12 hours of detection. Significant cyber-attacks are to be reported to CareCERT immediately following detection.
7	A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum with a report to senior management.
8	No unsupported operating systems, software or internet browsers are used in the IT estate
9	A strategy is in place for protecting IT systems from cyber threats, based on a proven security framework such as Cyber Essentials. This is reviewed at least annually.
10	IT suppliers are held accountable via contracts for protecting the personal confidential data they are process and for meeting the National Data Guardian's data security standards.

4.0 THE HUMAN RIGHTS ACT 1998 (HRA)

4.1 The HRA states that everyone has the right to respect for his private life and family life, his home and his correspondence. It also states there shall be no interference by a public authority with exercise of this right except as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country for the prevention of crime and disorder, for the protection of health, morals or for the protection of the rights and freedoms of others.

4.2 Further information about this or any other relevant legislation can be found at the Office of Public Sector Information website (www.opsi.gov.uk).

5.0 THE COMMON LAW DUTY OF CONFIDENTIALITY

5.1 The Common Law Duty of Confidentiality requires that unless there is a statutory requirement to use information that has been provided in confidence, it should only be used for purposes that the individual has been informed about and there is a legal basis to do so, or where there is an overriding public interest. The duty is not absolute but should only be overridden if the holder of the information can justify disclosure as being in the public interest i.e. to protect others from harm. If staff are unsure, they should seek advice from their line manager prior to disclosing any information.

6.0 CONFIDENTIALITY: NHS CODE OF PRACTICE

6.1 All staff are to abide by the Confidentiality: NHS Code of Practice. The full document can be viewed at https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

7.0 ACCESS TO HEALTH RECORDS ACT 1990

7.1 The Access to Health Records Act applies to requests to access the medical records of deceased patients and only to those entries entered into the case notes on or after 1st November 1991. Access may be granted to records made earlier than 1st November 1991 in certain circumstances, if they are necessary to make intelligible any part of the later records to which access is granted.

7.2 To access records under the Access to Health Records Act 1990 please see the Access to Health Records Policy on Flo. Further information is also provided in the "What happens to personal information held about you" also available on Flo.

8.0 DATA SECURITY AND PROTECTION TOOLKIT

8.1 The Data Security and Protection Toolkit is an online self-assessment mandated by the Department of Health and Social Care (DHSC). The Toolkit draws together legislation and central guidance set out by DH policy and presents them in a single standard as a set of information governance requirements, also known as assertions.

8.2 KCHFT are required to carry out self-assessments of their compliance against the following IG requirements:

- Management structures and responsibilities (e.g. assigning responsibility for carrying out the IG assessment, providing staff training, etc.)
- Confidentiality and data protection.
- Information and Cyber security

8.3 The purpose of the assessment is to enable organisations to measure their compliance against the requirements to see whether information is handled correctly and protected from unauthorised access, loss, damage and destruction. Where non-compliance is revealed, organisations must take appropriate measures, (e.g. assign responsibility, put in place policies, procedures, processes and guidance for staff), with the aim of making cultural changes and raising information governance standards through year on year improvements.

8.4 The ultimate aim is to demonstrate that the organisation can be trusted to maintain the confidentiality and security of personal information. This in-turn increases public confidence that 'the NHS' and its partners can be trusted with personal data.

9.0 KEY SENIOR ROLES

9.1 Chief Executive

9.1.1 The Chief Executive has overall responsibility for all aspects of the management of this policy.

9.1.2 The Chief Executive has appointed the Chief Finance Officer with overall executive leadership for Information Governance.

9.1.3 On behalf of the Chief Executive the Chief Finance Officer will establish clear lines of accountability arrangements for IG, which includes setting up a group to discuss IG, members of which will include senior managers and representative personnel from appropriate sectors of KCHFT.

9.2 Data Protection Officer (DPO)

9.2.1 The Data Protection Officer is the Director of ICT.

9.2.2 The Data Protection Officer will:

- report directly to the highest management level of the organisation;
- ensure timely involvement in all data protection issues;
- ensure the role is adequately supported by the necessary resources and is able to maintain expertise;
- not be pressurised by the organisation as to how to perform his or her tasks, and is protected from disciplinary action when carrying out those tasks;
- ensure there is no conflict of interest with any other role held.
- Undertake specialist DPO training 3-yearly

9.3 Senior Information Risk Owner (SIRO)

9.3.1 The Senior Information Risk Owner is the Chief Finance Officer.

9.3.2 The SIRO will:

- act as an advocate for information risk on the Board;
- take responsibility for the information risk process;
- review and agree actions in respect of information risks;
- ensure the trust's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff;
- provide written advice to the Chief Executive on any significant information risks reported; and
- undertake specialist SIRO training 3-yearly

9.4 Caldicott Guardian (CG)

9.4.1 The Caldicott Guardian is the Chief Medical Officer.

9.4.2 The Caldicott Guardian will:

- be responsible for agreeing, monitoring and reviewing internal protocols governing access to and use of patient identifiable information by staff within KCHFT, in compliance with UK legislation and national policy and guidance

- ensure the data protection work programme is successfully co-ordinated and implemented
- ensure that the organisation undertakes the monitoring and auditing of access to confidential information
- ensure KCHFT complies with the Caldicott principles and the principles contained within the Confidentiality: NHS Code of Practice, and that staff are made aware of individual responsibilities through policies, procedures and training
- provide routine reports to the Board regarding information sharing issues;
- maintain a log of all requests received and responses given relating to the Caldicott function; and
- undertake specialist Caldicott training 3-yearly training.

9.5 Organisational Responsibilities

9.5.1 This policy applies to all staff whether permanent, temporary, locum, bank, volunteers or contractors employed directly or working on behalf of Kent Community Health NHS Foundation Trust (KCHFT).

9.5.2 KCHFT have a duty to ensure that personal confidential data is used lawfully and that those undertaking work on behalf of KCHFT do so in a lawful manner.

9.5.3 The trust will take all reasonable steps to protect data which if breached could cause harm or distress to patients and staff, and damage to the trust's reputation or financial loss. The trust has a responsibility to put in place robust controls to protection confidentiality, integrity and availability of all systems.

9.5.4 To meet these obligations KCHFT must ensure that the contracts of permanent, temporary and locum staff contain clauses that clearly identify responsibilities for confidentiality, data protection and information security and must take reasonable steps to vet all staff before permitting them access to systems and information.

9.5.5 KCHFT will maintain an information asset register managed by the Information Asset Owners (IAOs).

9.5.6 KCHFT staff must comply with all aspects of the law that are concerned with the processing of personal confidential data. This includes legislation (Acts of Parliament), regulations, common law duties and professional codes of conduct.

9.5.7 KCHFT will establish the management structure for good practice to manage data effectively and respect personal privacy within KCHFT.

9.5.8 KCHFT will issue and regularly review a Confidentiality Code of Conduct that provides staff with clear guidance on the disclosure of business confidential / personal confidential data.

9.5.9 KCHFT staff will conduct Data Protection Impact Assessments (DPIAs) in accordance with data protection legislation and all high risk projects will be discussed with the Information Commissioners Officer (ICO) prior to commissioning.

9.5.10 KCHFT will undertake an annual review of its Data Flow Mapping process with the support of all service leads.

9.5.11 KCHFT staff will report all incidents on Datix and Serious incidents in accordance with national guidance and legislation.

9.5.12 KCHFT will ensure cyber security awareness is raised and policies are in place to support staff, further information can be found in the Cyber and Network Information Systems policy.

9.5.13 KCHFT will take actions as necessary to comply with the legal and professional obligations set out in the Records Management Code of Practice

9.5.14 All NHS records, and those of NHS predecessor bodies, are public records under the terms of the Public Records Act 1958. The Act sets out broad responsibilities for everyone who works with such records, and provides guidance and supervision by the Keeper of Public Records.

9.5.15 The Freedom of Information Act 2000 applies to all public records. Requests for information must be met within 20 days of the receipt of a request. Personal confidential data is exempt from disclosure under Freedom of Information (FoI). For further information refer to the organisations 'Freedom of Information Act 2000 Policy'.

9.6 Manager Responsibilities

9.6.1 All KCHFT managers will:

- ensure the appropriate screening checks and vetting controls are applied during the recruitment and selection process;
- ensure all staff have completed a new starter induction when joining the team;
- ensure they, and their direct reports, are compliant with all relevant legislation, national guidance, best practice and this policy;
- ensure all those undertaking work in the service are aware of their responsibility to maintain confidentiality of information relating to patients and staff at all times;
- ensure they, and their direct reports, adhere to the Data Protection, Caldicott and National Data Guardian principles at all times;
- ensure they, and their direct reports, uphold at all times individuals' rights within the law;
- develop appropriate local induction / training programmes, ensuring all staff are appropriately trained and aware of their responsibilities;
- ensure job descriptions contain responsibilities for IG, specific to that role;
- ensure all staff read, understand and sign their Confidentiality Code of Conduct;
- ensure all staff receive appropriate training on legislation and best practice, and are aware of their responsibilities with regard to information sharing, prior to accessing systems and information;
- determine required access levels to specific systems ensuring no unauthorised access is permitted;
- ensure the quality of information used
- ensure annual review and mapping of all data flows for the service.
- be responsible for the operational management of information sharing;
- ensure that any staff using personal confidential data for secondary purposes are authorised to do so (refer to the Secondary Uses of Personal Data policy on Flo);

- ensure that all staff are aware of the need to conduct a mandatory Data Protection Impact Assessment for any new projects, initiatives or changes in process which involve processing of personal identifiable data;
- ensure personal information is not transferred abroad without suitable safeguard – a Data Protection Impact Assessment (see Flo) must be completed and approved by the Data Protection Officer and noted at the Information Governance Assurance Group prior to any information being sent
- ensure that incidents are reported and investigated in accordance with the Incident policy;
- lead on investigations affecting their service and take appropriate actions to put in place robust controls to avoid reoccurrence;
- ensure incident investigations are followed through to point of closure and lessons identified are shared throughout the organisation.
- support planned evaluations and reviews of IG and implement change where recommended by such evaluation or review;
- ensure that staff are aware that they may be asked to participate in IG Service reviews
- expedite responses to Freedom of Information and Subject Access requests as a priority;
- appoint an IG Link Worker for their service (the list of staff identified is held by the Information Governance team).
- take appropriate technical and organisational security measures to safeguard personal information.
- ensure clear procedures on processing business confidential / personal confidential data are in place, regularly evaluated and monitored.
- must not, under any circumstances, remove personal, confidential or business sensitive information from the network without prior authorisation.
- must not, under any circumstances, use personal, confidential or business sensitive information for personal or economical gain
- ensure completion of the Leavers Checklist form when members of staff leave the service which includes disabling access to the network and emails as well as returning all assets (equipment, access fobs/keys, ID badges, diaries etc.)

9.7 Staff Responsibilities

9.7.1 All employees undertaking work on behalf of KCHFT have a personal responsibility to:

- ensure compliance with all relevant legislation, national guidance, best practice and this policy;
- be aware of their responsibility to maintain confidentiality of information relating to patients and staff at all times;
- adhere to the data protection, Caldicott and data security principles at all times;
- uphold at all times individuals’ rights within the law;
- bring to their line managers attention any concerns or breaches of data protection or poor practice within the service immediately and report breaches on Datix;
- undertake annual IG training and any other training appropriate their role identified in their PDP
- report immediately any breaches of confidentiality. Staff are personally responsible for ensuring that all their training remains valid

- abide by their staff groups professional standards and the Confidentiality Code of Conduct.
- manage securely in accordance with this policy all records created and/or handled including keeping appropriate records of their work and adherence to the record keeping standards.
- not, under any circumstances, remove personal, confidential or business sensitive information from the network without authority.
- not, under any circumstances, use personal, confidential or business sensitive information for personal or economical gain.

10.0 HOME, REMOTE AND MOBILE WORKING

10.1 Further information can be found on Flo:

- Home, Remote and mobile working standard operating procedure
- Working from Home Toolkit and associated documents
- The IG Do and Don't poster is also a useful guide to consider when working from home

11.0 TEMPORARY STAFF

11.1 Anyone undertaking work for, or with, the trust such as bank or agency staff, locums, students or volunteers must be advised about the trust's requirements for data security and protection (including record keeping) as part of their induction on arrival. It is the duty of the recruiting manager to ensure that such staff complete a local induction checklist and are made aware of their responsibilities for all areas of Information Governance.

12.0 THIRD PARTY CONTRACTORS

12.1 Contractors are expected to comply with this policy.

12.2 The manager of the contract is responsible for enforcing this position and monitoring compliance through regular meetings in line with the Contract Management policy.

12.3 Where information incidents or risks are reported by a third party contractor the Information Asset Owner and/or the contract lead must report the incident or risk immediately on Datix, in accordance with the Risk Management policy and Incident Policy.

13.0 TRAINING

13.1 Data Security and Protection Training

13.1.1 KCHFT mandatory training for all staff (new starters at induction and all other staff annually) includes:

- ***Data Security and Protection Training*** including Cyber Security (previously IG induction)
  Delivered via the Education and Development Portal, TAPs

13.1.2 Training needs are monitored by line managers through the mandated appraisal process. A gap analysis will be included during the review and required training, applicable to the individuals' role, will be documented.

13.1.3 It is the responsibility of the line manager, through the 1:1 and appraisal process to determine training needs for individual staff members.

13.1.4 All staff must receive appropriate systems training e.g. TAPS, before being given access to any live system.

13.1.5 NHS Digital is further developing the e-learning tool and supplementary modules will be published on Flo for managers to include as required in staff personal development plans considered essential to role.

13.2 Induction training

13.2.1 All new permanent staff joining the trust will have to attend the corporate induction. The Resourcing Team automatically book all new permanent starters onto the Corporate Induction programme.

13.2.2 Bank and other temporary staff will be expected to undertake IG training prior to their first assignment. This will be overseen by the Bank manager.

13.2.3 Once on site all staff will be inducted using the new starter induction checklist which will includes awareness of all policies and signing the Confidentiality Code of Conduct.

13.2.4 Further information, checklists and assessments are all available on Flo.

13.3 Annual mandatory refresher training assessment

13.3.1 All staff must undertake annual refresh of their Information Governance training. This can be completed via any of the following methods:

- Data Security and Protection training through TAPs
- the IG POD (face to face assessment)

13.4 Training for Specialist Roles

13.4.1 There are roles within the organisation which require specific training.

13.4.2 For example, the Senior Information Risk Owner, Caldicott Guardian, Data Protection Officer, Information Asset Owner and those staff in Information Governance and Cyber Security all have specific duties within their role which requires specialist knowledge.

13.4.3 In addition to any role specific training specialist roles must also complete the IG mandated module on NHS Digital e-learning annually.

13.4.4 For more information contact the IG team on 0300 123 2079 or log a call on the IT Service Portal (click on the Information Governance icon)

14.0 COMMUNICATION

14.1 IG Link Workers

14.1.1 Every service requires at least one link worker to support communication within their service for all matters relating to IG. This recommendation came from the Information Commissioner following an audit of processes in February 2015.

14.1.2 The Link Worker will support their service in addressing training concerns, disseminating information to all team members, overseeing the distribution of the IG newsletter and providing the IG team with details of concerns or issues from their Service.

14.1.3 If your service does not have a link worker ask your manager to nominate one today – call 0300 123 2079 or log a call on the IT Service Portal (click on the Information Governance icon)

14.2 IG Workspace

14.2.1 The IG team have a useful online resource called the IG Workspace on Flo. Membership is open and IG would request all staff join up to receive the monthly IG newsletter, updates, news and mandatory notifications of changes in law, best practice and sector specific guidance.

14.3 IG newsletter

15.3.1 The IG newsletter is released on a regular basis and is published in the IG Workspace on Flo.

15.0 INFORMATION GOVERNANCE ASSURANCE GROUP

15.1 The Information Governance Assurance Group (IGAG) is chaired by the DPO, SIRO or CG and is a sub group of the Corporate Assurance and Risk Management Group (CARM).

15.2 The IGAG provides a focal point for the resolution and/or discussion of IG issues, to report trends and to receive assurance from key leads on compliance.

16.0 CORPORATE ASSURANCE AND RISK MANAGEMENT (CARM) GROUP

16.1 The CARM is chaired by the DPO, SIRO or CG.

16.2 The objective of the CARM is to ensure the organisation identifies, manages and mitigates risk through the corporate risk register and Board Assurance Framework.

16.3 The IG team submit an exception report to every meeting which includes risks to be noted by the Senior Information Risk Owner.

16.4 High rated risks are escalated to the Executive Team for consideration for inclusion on the Board Assurance Framework.

17.0 INCIDENT AND RISK MANAGEMENT FOR INFORMATION GOVERNANCE

17.1 Management of Information Governance Incidents

17.1.1 All individuals undertaking work on behalf of KCHFT are responsible for recording on Datix all actual and near miss incidents involving any aspect of IG.

17.1.2 All individuals have a responsibility to report any observed or suspected weaknesses or threats to data protection, information security or software malfunction.

17.1.3 All IG incidents must be reported immediately and no longer than 24 hours after the event. If there is uncertainty as to whether an IG incident is to be categorised as "serious" then staff must speak to either the Patient Safety team and/or the Information Governance team.

17.1.4 All IG incidents are categorised by the IG team using the NHS Digital Guide to the Notification of Data Security and Protection Incidents

17.1.5 If an IG incident is considered significant, following the guidance above, it will be categorised as a Serious Incident and the IG team will support a full Root Cause Analysis investigation, with the authority of the Caldicott Guardian or Senior Information Risk Owner. If necessary, the Serious Incident may also be reported to the Information Commissioner's Office for review. This could have the potential for the trust to be fined if the ICO deems it necessary.

17.1.6 The IG team will work closely with the Incident Management Team to develop a reporting process which informs the organisation of all actual, near-miss and external incidents reported.

17.1.7 The report will be presented to the Corporate Assurance and Risk Management Group and the Information Governance Assurance Group. The in-depth analysis will evidence trends and `hot-spots` to enable additional support and training in areas of weakness to avoid repetition of breaches.

17.1.8 For further information see the Incident Policy on Flo.

17.2 Management of Information Risks

17.2.1 Information risk management is the process of understanding and responding to factors that may lead to a failure in confidentiality, integrity or availability of systems or data.

17.2.2 Information is a vital asset in the provision of high quality care and business process. It is integral to the governance, service planning and performance management of KCHFT.

17.2.3 The SIRO has overall responsibility for the management of information risks within the trust.

17.2.4 All risks which impact on the services ability to remain compliant with data protection legislation must be recorded on Datix and assessed in accordance with the Risk Management policy.

17.2.5 All risks recorded on Datix which are a risk to compliance with the data protection legislation must be recorded as an information governance risk for them to be included in the report discussed at the IGAG and CARM.

17.2.6 The SIRO is supported in their role by the Information Asset Owners (IAO) who are designated owners of key systems within the trust.

17.2.7 IAOs are responsible for ensuring all risks within their designated systems are appropriately managed, risks to breach of data protection legislation are mitigated and reported appropriately in line with the Risk Management policy.

17.2.8 The Cyber Security Specialist role will work with the IT Infrastructure Manager to provide assurance to the IGAG on the implementation of security measures and management processes to protect trust vital assets against the effect of malicious software and other risks.

17.2.9 Significant risks must be reported to the Patient Safety team immediately and recorded on Datix. Advice and support can also be obtained from the Information Governance team and the SIRO.

17.2.10 All trust-wide IG risks are recorded using the electronic management tool Datix. A full and comprehensive list of risks together with controls for mitigation is available on request.

17.2.11 All IG risks are managed and monitored by the Information Governance Assurance Group on a regular basis.

17.2.12 Significant IG risks will be highlighted to the Corporate Assurance and Risk Management Group.

18.0 INFORMATION GOVERNANCE SERVICE REVIEWS

18.1 The trust must ensure that it handles personal information appropriately and therefore control mechanisms have been put in place to manage and safeguard the security and confidentiality of information that the trust handles.

18.2 IG Service reviews focus on controls within electronic records management systems, but will also include paper record systems and general security of information within the workplace environment. The purpose is to discover whether security or confidentiality has been breached, or put at risk as a result of weak, non-existent or poorly applied controls.

18.3 Every service can request an internal IG Service review to be conducted. The review consists of an in-depth self-assessment questionnaire, if necessary, a visit to site to conduct a visual review and a comprehensive report with an opinion on the level of compliance.

18.4 Each year approximately 12 services will be targeted for mandatory IG Service reviews based on incidents and risks reported or following a significant event requiring further investigation.

18.5 If your service requires an IG Service review please contact the IG team.

19.0 DATA PROTECTION AND CONFIDENTIALITY

19.1 Confidentiality Code of Conduct

19.1.1 The KCHFT Confidentiality Code of Conduct can be found on Flo.

19.1.2 The code of conduct must be signed by all individuals undertaking work for KCHFT. It can also be signed by third party organisations to support the standard NHS terms and conditions of contract.

19.1.3 Managers have a responsibility to ask all individuals to sign the Confidentiality Code of Conduct as part of their local induction as soon as they commence working with their Service. A copy of the signature page must be kept in the staff personal file for audit purposes.

19.1.4 Managers who appoint third party contractors are responsible for ensuring the Confidentiality Code of Conduct is signed as part of service delivery if personal confidential information is being processed.

19.2 Data Protection Impact Assessments (DPIAs)

19.2.1 Data Protection Impact Assessments (DPIAs) are a tool which can help identify the most effective way to comply with data protection obligations and meet individuals' expectations of privacy. An "individual" in the context of completing a DPIA includes patients, carers, staff and anyone working on behalf of KCHFT. An effective DPIA will allow KCHFT to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

19.2.2 The Department of Health currently mandates DPIAs to be completed and together with the Information Commissioner's Office, DPIAs are promoted as a tool which will help the trust to comply with DPA obligations, as well as bringing further benefits. Data Protection Impact Assessments are a legal requirement for high risk data flows.

19.2.3 Key Points:

- A DPIA is a process which assists in identifying and minimising the privacy risks of new projects or policies.
- Conducting a DPIA involves working with people within KCHFT, with partner organisations, and if necessary, with the public to identify and reduce privacy risks
- The DPIA will help to ensure that potential problems are identified at an early stage, when addressing them will often be simpler and less costly.
- Conducting a DPIA should benefit by producing better policies and systems and improving the relationship between organisations and individuals
- It is a legal requirement for the trust to liaise with the ICO for any high risk processing

19.2.4 All purchases of new systems which are likely to be used to process personal confidential data must only be commissioned once a DPIA has been completed.

19.2.5 All purchases of hardware or software must be with the authority of the IT service and all information security controls documented as part of the DPIA.

19.2.6 KCHFT will only permit approved software to be installed on its devices / network and all new requests must be authorised by the IT Service Centre.

19.2.7 The DPIA template can be requested from the IG team by logging a call on the IT Service Centre (Corporate Operations icon).

19.2.8 All DPIAs (draft or completed) remain the responsibility of the Service completing them. IG provide a reviewing service, and organise sign off. Any draft DPIAs will be held by the IG team for a period of 6-months and if not completed will be escalated to the appropriate senior manager within the Service.

19.3 Data Flow Mapping (DFM)

19.3.1 Transfers of information between the trust's departments and sites, other NHS organisations, Local Authorities with Social Service Responsibilities or other third parties are commonplace and may be achieved using a variety of transfer means and formats (i.e. digital and hardcopy). It is a legal responsibility of the trust to ensure that transfers of personal information for which they are responsible are secure at all stages.

19.3.2 The loss of personal information will result in adverse incident reports which will not only affect the reputation of the organisation but, in the case of disclosing personal information intentionally or recklessly, is also a criminal offence.

19.3.3 To ensure all transfers are identified Services will need to carry out an audit of transfers. This is known as Data Flow Mapping and the register provided by this exercise identifies the higher risk information transfers which need to be managed.

19.3.4 Reports of any high risks will be reported to the Senior Information Risk Owner by the Information Governance Team.

19.3.5 The data flow mapping template can be found on Flo

19.4 Information Sharing

19.4.1 Under the NHS Care Record Guarantee, when providing healthcare, patients must be informed that staff will share their health record with the people providing care or checking the quality of care – see the patient leaflet "What happens to personal information held about you?".

19.4.2 Caldicott Principle 7 states that the duty to share information can be as important as the duty to protect patient confidentiality. Staff must have the confidence to share information in the best interests of patients within the framework set out by the Caldicott Principles.

19.4.3 Staff must ensure that they comply with the General Data Protection Regulation and the UK Data Protection Act 2018 and use the Caldicott Principles where appropriate. Further information can be found on Flo:

- Safe haven guidance
- How to share information – Caldicott Principles
- How to share information with the Police
- How to share information for direct care flowchart
- Information Sharing Agreement (and associated Standard Operating Procedure and guidance notes)

19.4.4 If staff have concerns over sharing information, or if they are experiencing any barriers to sharing person identifiable information, they should speak to their line manager in the first instance.

19.5 Legal Basis for processing / sharing information

19.5.1 The trust has a legal obligation to provide certain healthcare services (those which we are commissioned to provide) and under our authorisation as an NHS Foundation Trust we are to provide goods and services for the purposes of the health service in England. When we engage with a patient we establish, and then owe to them, a duty of care and, in satisfying that duty, we must make an adequate record. In order to provide safe, holistic care and fulfil our duty of care to our patient, it is sometimes necessary to share part or all of the information contained in that record with other professionals involved in the patient's care. See How to share information (Caldicott Principles) on Flo.

19.5.2 Clinicians have a legal obligation to share information when processing is necessary to perform our task as a health provider. For example, processing may be necessary for medical diagnosis, provision of health and care treatment (subject to certain safeguards).

19.5.3 The following applies for staff and patient information.

19.5.4 For processing personal information (not confidential) the following legal bases may apply:

Article 6 (1) (a) – the data subject has given consent to the processing of his or her personal data for one or more specific purposes **(*this is not to be used for processing and sharing patient information as the trust can rely on another legal basis*)**

Article 6 (1) (b) – processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract

Article 6 (1) (c) - processing is necessary for compliance with a legal obligation to which the controller is subject;

Article 6 (1) (d) - processing is necessary in order to protect the vital interests of the data subject or of another natural person; ***(life and death situations)***

Article 6 (1) (e) - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

Article 6 (1) (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

19.5.5 For processing personal information (confidential) the following legal bases may apply:

Article 9 (2) (a) – the data subject has given explicit consent to the processing of those personal data for one or more specified purposes

Article 9 (2) (b) – processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law

Article 9 (2) (c) - processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

Article 9 (2) (f) - processing is necessary for the establishment, exercise or defence of legal claims

Article 9 (2) (g) - processing is necessary for reasons of substantial public interest

Article 9 (2) (h) - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

Article 9 (2) (i) - processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

19.5.6 The basis for processing the information should be recorded e.g. in the patient notes / staff file.

Processing information includes:
Obtaining
Holding
Using
Recording
Sharing
Deleting

In short, everything we do with information.

19.5.7 Clinicians **must no longer ask patients for consent** to share their information for direct patient care as consent gives patient's rights which the trust cannot comply with. However, they must still inform patients who they will be sharing the information with and why.

19.5.8 If a patient objects to particular personal information being shared for their own care, you must not disclose the information unless it would be justified in the public interest i.e. Section 42 of the Care Act 2014 or Sections 17 or 47 of the Children Act 1989 in regard to safeguarding adults or children.

19.5.9 You can also disclose the information if the sharing is of overall benefit to a patient who lacks the capacity to make the decision (GMC Confidentiality: good practice in handling patient information).

19.5.10 To help with explaining this to patients there is a leaflet published by KCHFT and held on the public website. This leaflet needs to be made available to patients at the **first point of contact with KCHFT and recorded on the patient record**. The leaflet contains details about why we collect information, the legal basis for doing so and how long we will keep the information. It also provides guidance about how to complain if they are not happy with how their personal information has been used or protected.

19.6 Privacy Poster

19.6.1 The Data Protection Act (DPA) provides a general requirement for individuals to be informed about how personal information relating to them is used and shared – this is termed ‘fair processing’. Where the personal information concerned is confidential in nature the steps that must be taken to ensure that individuals are effectively informed are more demanding. In addition, the DPA and the common law of confidentiality and Department of Health policy provide individuals with rights in respect of such data which individuals must also be informed about.

19.6.2 The trust has two ways to inform patients of what we do with the information that it collects about them which can be found on the public website:

19.6.3 The link to the Privacy Poster on the Privacy page of the patient website
Patient leaflet – What happens to personal information held about you?

19.6.4 All staff must ensure that the poster and leaflet are prominently displayed in waiting areas where patients visit, and be available on request.

19.6.5 In order to satisfy our legal obligation, patients must be given a copy of the patient leaflet above at the first contact (or as soon as possible thereafter) with the trust. Patients only need to be informed once and so when a leaflet is given, this must be recorded in their patient record.

19.7 Subject Access Requests (SAR)

19.7.1 All SARs for clinical and non-clinical information are managed by the Legal Team department. Details of what constitutes an SAR can be found on Flo and in the Access to Health Records policy.

19.7.2 The Legal Team can be emailed on kcht.legal@nhs.net and further guidance is provided in the Access to Health Records policy on Flo.

19.7.3 Full details are given in the patient leaflet "What happens to personal information held about you" which is available on the Kent Community Health NHS Foundation Trust website.

19.8 Using clinical data for non-clinical purposes (secondary uses)

19.8.1 It is generally recognised in the NHS that it is acceptable and legal for patient confidential data to be used to deliver safe and effective care to patients. This includes the audit and assurance of the quality of that care. These uses of data are known as 'healthcare medical purposes' or 'primary uses'. However, there are many uses of data within the NHS that are not directly related to patient care, such as performance management and planning, and the payment of invoices. These uses are regarded as 'non-healthcare medical purposes' or 'secondary uses'.

19.8.2 It is not acceptable to use personal data for non-clinical purposes unless there is a legal basis to do so. Staff must also make clear what rights the individual has open to them, including any ability to actively dissent.

19.8.3 For further information please view the Secondary Use of Personal Data policy on Flo. If in any doubt about the use of data within your service or questions regarding best practice contact the Performance team kcht.performanceteam@nhs.net who will be able to advise you.

19.8.4 The policy is based on the document 'Implementing the ICO Anonymisation Code of Practice' providing guidance to Health and Care services on disseminating data into controlled environments. The document outlines the need for consistent use of patient identifiers and the importance of reducing the risk of re-identification to a sufficiently low and acceptable level.

19.8.5 Further details are given in the patient leaflet "What happens to personal information held about you?" which is available on the Kent Community Health NHS Foundation Trust website.

19.9 Transfers of data outside the EEA

19.9.1 KCHFT is responsible for the security and confidentiality of personal confidential data it processes. Processing may include the transfer of information to countries outside the European Economic Area (EEA). Where this is the case a transfer must not be made unless that country has an adequate level of protection for the information and for the rights of individuals.

19.9.2 KCHFT's registration with the Information Commissioner states that it transfers personal confidential data outside the EEA, as some services do this with third parties working on our behalf. KCHFT Services must regularly review the flows of patient and personal confidential data from KCHFT to understand whether any such information flows outside of the EEA, and notify the Information Governance team accordingly.

19.9.3 Decisions on whether to transfer personal confidential data must only be taken after a Data Protection Impact Assessment (DPIA) has been completed, and all the relevant risks to an individuals' privacy have been signed off by the Senior Information Risk Owner. The DPIA template can be requested from the IG team..

20.0 INFORMATION SECURITY

20.1 Data stored in computer systems represents an increasingly valuable asset to the trust as its systems expand and increased reliance is placed on them.

20.2 KCHFT has legal obligations to maintain high security levels as defined in the Data Protection Act, the Network and Information Systems Regulations 2018, the Computer Misuse Act 1990 and all other associated legislation and best practice, including the National Data Guardian's data security principles.

20.3 The main objective is to preserve:

Confidentiality – data and file access is confined to those with specified authority to view the data;

Integrity – information shall be complete and accurate. All system, assets and networks are operating correctly according to specification; and

Availability – information shall be available and delivered to the right person at the time when it is needed

20.4 KCHFT will do this by ensuring:

- computer systems are properly assessed for security;
- confidentiality, integrity and availability are maintained;
- staff are aware of their responsibilities, roles and accountability;
- procedures to detect and resolve security breaches are in place; and
- the trust is able to continue its activities in the event of an Information security breach.

20.5 Personal confidential and business sensitive data can be processed in many different ways, which include but are not limited to being:

- stored on databases
- stored on computers
- transmitted across internal and public networks
- printed or hand written on paper, white boards etc.
- sent electronically e.g. by email
- stored on removable media such as CDs, Memory sticks, hard disks, tapes etc.
- stored on fixed media such as hard disks and disk sub-systems
- held on film or microfiche
- presented on slides, overhead projectors, using visual and audio media
- spoken during telephone calls and meetings or conveyed by any other method

20.6 Data Encryption

For further information refer to the Cyber, Network and Information Systems policy on Flo.

20.7 Audio Visual Recording

Please see the Audio Visual Recording Protocol on Flo.

20.8 Encrypted USB Media

For further information refer to the Cyber, Network and Information Systems policy on Flo.

20.9 Email and Website Monitoring

For further information refer to the Cyber, Network and Information Systems policy on Flo.

20.9.1 **Do not assume e-mail is private:** messages are constantly being monitored for viruses and also they can be intercepted or wrongly addressed, and can be easily forwarded to unknown third parties. Even deleted messages may be retrieved, or traced via back-up copies.

20.9.2 KCHFT is ultimately responsible for all business communications. Emails are written communication and are accessible and open to scrutiny in the same way that any other written communication is. Email communication is also accessible under the Freedom of Information Act. Do not write personal or derogatory remarks in email communication.

20.9.3 For further information refer to the Cyber, Network and Information Systems policy on Flo.

20.10 Internet use filtering

For further information refer to the Cyber, Network and Information Systems policy on Flo.

20.11 Password Management

For further information refer to the Cyber, Network and Information Systems policy on Flo.

20.12 System Access

For further information refer to the Cyber, Network and Information Systems policy on Flo.

20.13 Network Information Security (NIS) Regulations

Further information on this legislation and the framework of requirements the trust has to comply with is available in the Cyber and Network Information Systems policy on Flo.

20.14 Virus Protection

For further information refer to the Cyber, Network and Information Systems policy on Flo.

20.15 CareCERT

For further information refer to the Cyber, Network and Information Systems policy on Flo.

20.16 Cyber Essentials

KCHFT are working towards full Cyber Essentials accreditation. For further information contact the Cyber Security Specialist – see contact list.

20.17 IT Equipment and Media Disposal

20.17.1 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.

20.17.2 Under no circumstances must you dispose of any equipment without following the process outlined in the Cyber and Network Information Systems policy on Flo.

20.18 Digital Forensic Readiness

20.18.1 Forensic readiness is the capability of KCHFT to make use of digital evidence when required to support investigations.

20.18.2 A forensic investigation if digital evidence is commonly used as a post event response to a serious IG incident. However, there are many other circumstances where an organisation may benefit from the ability to gather and preserve digital evidence.

20.18.3 Any suspected inappropriate usage of computer equipment should be reported immediately to the line manager, if appropriate, and the IT Service Centre.

20.18.4 Inappropriate usage of computer equipment/system can be anything deemed to be in breach of the Cyber and Network Information Systems policy.

20.18.5 Contact the IT Service Centre immediately on 0300 123 1885.

20.18.6 For further information refer to the Cyber, Network and Information Systems policy on Flo.

20.19 Lost or Stolen Equipment

20.19.1 Theft or suspected theft must be reported to the relevant manager immediately.

20.19.2 A call must be logged with the IT Service Centre to ensure the device is disabled or locked.

20.19.3 The Police must also be contacted and a crime reference obtained.

20.19.4 An incident must be raised on Datix and a management investigation undertaken.

20.20 Damaged or Faulty equipment

For further information refer to the Cyber, Network and Information Systems policy on Flo.

20.21 Compromised Access Controls

20.21.1 This is a serious breach of information security and must be reported immediately to the IT Service Desk and reported on Datix. If significant you must also notify the

Patient Safety team immediately. For further information refer to the Serious Incident policy on Flo.

20.21.2 All passwords must be changed immediately.

21.0 RECORDS MANAGEMENT

21.1 Information is the lifeblood of the trust and without it the organisation cannot function effectively.

21.2 Records are defined as ‘recorded information, in any form, created or received and maintained by the trust in the transaction of its business or conduct of affairs and kept as evidence of such activity’.

21.3 This section refers to all records, health and corporate operational records, held in any format. These include, but are not limited to:

- all administrative records including databases and emails (e.g. personnel, estates, financial and accounting records, notes associated with complaints); and
- all clinical records for all specialties (including clinical systems records, x-ray, audio and video files, imaging reports, registers, diaries, team communication books, etc.)
- Messages and recorded conversations from MS Teams and other instant messaging systems (including mobile phones).

21.4 Records Management is a discipline which utilises an administrative system to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally sound, whilst at the same time serving the operational needs of KCHFT and preserving an appropriate historical record. The key components of records management are:

- record creation;
- record maintenance (including tracking of record movements);
- access and disclosure;
- appraisal;
- archiving; and
- disposal

21.5 The purpose of this section is to ensure that records management systems and practice throughout KCHFT comply with relevant legislation, professional and Information Governance standards.

21.6 Information is a corporate asset. KCHFT records are important sources of administrative, evidential and historical information. They are vital in supporting its current and future operations (including meeting the requirements of Data Protection and Freedom of Information legislation), for the purpose of accountability and for an awareness and understanding of its history and procedures.

21.7 Proper management of records is fundamental to the business of the organisation. KCHFT records are its corporate memory, providing evidence of actions and supporting decision making whilst supporting its daily functions and operation.

21.8 Records support consistency, continuity, efficiency and productivity. The organisational benefits of sound records management are:

- control and availability of valuable information assets
- good utilisation of storage and server space
- compliance with legislation and standards
- efficient use of staff time
- reduced costs

21.9 Clinical records and the information they contain are vital to the satisfactory treatment and care of patients. The importance of records management and good record-keeping include:

- helping to improve accountability
- showing how decisions related to patient care were made
- supporting the delivery of services
- supporting effective clinical judgments and decisions
- supporting patient care and communications
- supporting the involvement of the patient in their own health care
- making continuity of care easier
- providing documentary evidence of services delivered
- promoting communication and sharing of information between members of the multi-professional healthcare team
- helping to identify risks, and enabling early detection of complications
- supporting clinical audit, research, allocation of resources and performance planning
- helping to address complaints or legal processes

21.10 KCHFT has a responsibility to ensure that the healthcare each patient receives is recorded appropriately and that records are processed responsibly to support high quality care. There are professional standards for clinical record-keeping which are part of requirements for professional registration. For further information refer to the Clinical Record Keeping Policy.

22.0 RECORDS MANAGEMENT STRATEGY STATEMENT 2023-2026

22.1 Most services have now moved to completely electronic records but a small number are still reliant on paper records. Over the next 3 years, the trust will continue its move to predominantly electronic records across both clinical and corporate services. This will support the trust in providing a more efficient and responsive service and help align to the NHS' paperless 2023 agenda. Scanning is not a viable option for historical paper records to be retained. In some cases, these will be moved to the trust's central archiving facility as the most efficient option for both managing such records and use of the trust's Estate.

22.2 Aims of the KCHFT records management system

The aims of the KCHFT records management systems (electronic and paper) are to ensure:

22.3 Accountability

Records are adequate to account fully and transparently for all actions and decisions, in particular to:

- protect legal and other rights of staff or those affected by those actions;
- facilitate audit or examination;
- provide credible and authoritative evidence

22.4 Availability

KCHFT is able to service its business needs and comply with legislative requirements.

22.5 Accessibility

Those with a legitimate right can access records, and the information within them is located and displayed in a way consistent with its initial use, and the current version is identified where multiple versions exist. The information must be able to be read or received and understood by the individual or group which it is intended for. Support must be given to enable effective, accurate dialogue between a professional and a service user – see the Accessible Information Standard on Flo

22.6 Interpretation

The context of the record can be interpreted i.e. identification of staff who created or added to the record and when, during which business process, and how the record is related to other records.

22.7 Quality of records

Records are complete and accurate and reliably represent the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated.

22.8 Performance measurement

The application of records management procedures are regularly monitored against agreed indicators and action taken to improve standards as necessary.

22.9 Staff training

All staff are made aware of their responsibilities for records management.

22.10 Security of records

To ensure:

- the security from unauthorised or inadvertent alteration or erasure
- access and disclosure are properly controlled and;
- there are audit trails to track all use and changes in order to ensure that records are held in a robust format which remains readable for as long as records are required.

22.11 Record creation and maintenance

22.11.1 Records created by KCHFT should be arranged in a record-keeping system that will enable quick and easy retrieval of information to support the business of the organisation, ensure informed care of patients and in order to respond to requests for information under the Freedom of Information Act, Data Protection Act, Access to Health Records Act and Environmental Information Regulations.

22.11.2 High quality information underpins the delivery of high quality evidence based healthcare. Clinical records must therefore be complete and accurate and healthcare staff must adhere to the record keeping standards the Clinical Record Keeping Policy.

22.12 Electronic records

22.12.1 KCHFT will consider electronic records management systems to improve the efficiency and accessibility of its records. The principles within this policy apply equally to the lifecycle of an electronic record. However, the qualities of availability, accessibility, interpretation and trustworthiness must be maintained for as long as the record is needed, perhaps permanently, despite changes of format.

22.12.2 There are essentially two types of electronic records:

- those that are created electronically e.g. Electronic patient record, reports, spreadsheet and e mails
- those that are copied or scanned from paper format

22.12.3 Documents (or data files) may also be created by an electronic records management system (ERMS) itself, by its users or may be imported into it.

22.12.4 KCHFT must have a documented and approved operating procedure manual for each ERMS it uses. This manual will provide the evidence that the processes for ensuring authentic documents are robust. If an electronic document is ever challenged this manual will demonstrate that the processes are precise, secure and approved.

22.12.5 The Records Management Code of Practice provides guidance in relation to ‘Digital Records, Digital Continuity, Digital Preservation and Forensic Readiness’ and refers specifically to the Digital Preservation Handbook. It is recommended that the Records Management Code of Practice and this handbook are referred to at the procurement stage of any electronic software to ensure the integrity of digital records.

22.13 NHS Number

22.13.1 The NHS Number is the only national unique patient identifier used to help healthcare staff and service providers match the patient to their healthcare records. Almost everyone registered with the NHS in England and Wales has their own unique NHS Number.

22.13.2 The NHS Number should be used as the prime identifier for all KCHFT patients. It should be included on electronic records, wristbands, notes, forms, letters, documents, reports and onward referrals which include personal confidential data and are used for that person’s care. Sexual Health is an exception since the data is kept separate from other healthcare information. Please refer to the trust's Clinical Record Keeping Policy.

22.13.3 The NHS Number should be captured at the earliest point that a patient presents to a KCHFT service; as soon as possible after first contact and before or at the start of an episode of care. Where the NHS Number is not available then tracing should be performed as early as possible in the episode either at point of contact or as a back-office process. The Summary Care Record (SCR) should be used to trace NHS Numbers.

22.14 Storage and transportation

22.14.1 For legal and practical reasons records must be stored and transported securely. Paper records must be stored and handled securely to maintain confidentiality and integrity even at a non-KCHFT site such as a school, college, university or GP surgery. You must mark the cabinets accordingly. See Transport paper clinical and staff records and associated Checklist for Information Held at a Non-KCHFT Site.

22.14.2 Physical storage must also conform to Fire and Health and Safety regulations to protect staff and maintain records in good condition.

22.14.3 Whilst clinical records and/or staff records are in use, the person using them is responsible for maintaining the security of the record whilst it remains in their custody.

22.15 Patient and parent held notes

22.15.1 Where patients and / or parents hold their own, or their child's, records they must be made aware of the importance of these records for health care professionals and the need to keep them safe. They must also be made aware that these records are an official health record and as such will need to be returned to the trust when requested.

22.16 Scanning paper records

22.16.1 The need to reduce costs across KCHFT has seen a move in some teams to consider scanning paper records to both free up valuable storage space and reduce the cost of archiving paper records for years. Before a decision is made to scan records into an electronic medium and destroy the originals, consideration must be given to:

- the costs of the initial set up, ongoing scanning and then any later media conversion, bearing in mind the relevant retention period for the record;
- the need to protect the evidential value of the record by copying and storing the record in accordance with British Standard – Code of Practice for Legal Admissibility and evidential weight of information stored electronically (BIP0008); and
- whether the records are of any archival value and there needs to be consultation prior to destruction.

22.16.2 In the event that scanning is discussed within your Service, the scanning procedure available on Flo must be followed. Advice should also be sought from the Director of ICT. All contact details can be found on Flo.

22.16.3 Should a service decide to outsource the scanning of records; the procurement and contracts teams must be consulted to ensure robust contracts are in place.

22.17 Maintenance through time

22.17.1 For records in digital format, maintenance in terms of back-up and planned migration to new platforms must be designed and scheduled to ensure continued access to readable information. The qualities of availability, accessibility, interpretation and trustworthiness must be maintained for as long as the record is needed, perhaps permanently, despite changes of format.

22.17.2 The Digital Preservation Handbook is an important tool to enable the trust to address digital continuity (continued availability of electronic data), digital preservation (data remains accessible and useable) and forensic readiness (to gather, protect and analyse digital evidence to support investigations) of the electronic systems purchased/used.

22.18 Documentation of controlled drugs

Please refer to the trust's Medicines Management policies.

22.19 Transfer of care/Deteriorating Patient

Please refer to the trust's Transfer of Care Policy and/or the Deteriorating Patient Standard Operating Procedure.

22.20 Appraisal, archiving and disposal

22.20.1 Appraisal of records held in any format should be undertaken by staff with appropriate training and understanding of the operational area to which the record relates. Retention dates will be determined with reference to the Records Management Code of Practice which is available on Flo. For electronic records, good housekeeping of both shared and personal drives is essential to remove material that should no longer be retained this includes email (which should be deleted on a regular basis).

22.20.2 Permanent preservation of records held in any format will be undertaken in consultation with the Information Governance team, Information Governance Assurance Group and in conjunction with KCHFT's approved place of deposit.

22.20.3 Appendix 2 of the Records Management Code of Practice outlines the types of records that are to be preserved or should be considered for preservation. As an absolute minimum the following records are to be preserved and transferred to a place of deposit:

- Board meetings (held in public and closed meetings)
- Chief Executive Records
- Committees listed in the scheme of delegation or that report into the Board and major projects
- Final annual accounts report (if not transferred with the board papers

22.20.4 Paper records archived on local site must be stored in appropriate filing systems and kept clean, dry and free from contaminants. They should be stored so they are easily accessible, in an order to facilitate retrieval and must comply with current security and health and safety requirements.

22.20.5 The trust has an industry standard approved off-site archiving storage facility. Guidance for staff on the use of the archiving storage facility is available on Flo. All administration for this service is managed via the Information Governance team. For all matters relating to archiving, including document retention periods please call 0300 123 2079 or log a call on the IT Service Portal (click on Information Governance)

22.20.6 Electronic systems must be able to

- archive records when records are no longer active
- set retention periods aligned to the type of record concerned
- set destruction dates for individual records
- allow for information to be permanently deleted when the retention period is reached, unless the information has been selected for permanent preservation.

22.20.7 There should be no automatic deletion of electronic records as all records need to be appraised before deletion is authorised

22.20.8 Paper records which have reached their minimum retention period and have not been selected for permanent preservation should be destroyed in a secure and confidential manner – see Confidential Waste Disposal below. The retention period for some records may need to be extended in certain situations, which means destruction must be delayed. These situations are detailed in the Records Management Code of Practice and include:

- A record due for destruction is known to be the subject of a request for information,
- A record is known to be the subject of or potential legal action,
- A record is known to be the subject of an incident (both serious and non) serious)'
- A record is known to be the subject of a complaint. destruction must be delayed until disclosure has taken place.

22.20.9 The IG team will regularly publish on Flo lists of archived boxes due for destruction for Services to identify any records to be retained. The IG team will also regularly check and authorise destruction of records in the archiving storage facility (as a minimum, annually).

22.20.10 Paper clinical records can be disposed of in confidential waste bins as long as there is a record kept by the Service of what has been disposed of and when. Use the standard archiving contents list template on Flo. Contents sheets must then be retained for 25 years, aligned to the RM Code of Practice retention period for destruction certificates.

22.21 Disposal of electronic records

22.21.1 The ICO will adopt a realistic approach in terms of recognising that deleting information from a system is not always a straightforward matter and that it is possible to put information ‘beyond use’, and for data protection compliance issues to be ‘suspended’ provided certain safeguards are in place.

22.21.2 The trust will be satisfied that information has been ‘put beyond use’, if not actually deleted, provided that the information on the system holding it:

- is not able, or will not attempt, to use the personal data to inform any decision in respect of any individual or in a manner that affects the individual in any way;
- is not accessible to any other organisation;
- is surrounded with appropriate technical and organisational security, and;
- commits to permanent deletion of the information if, or when, this becomes possible.

22.21.3 The ICO will not require data controllers to grant individuals subject access to the personal data provided that all four safeguards above are in place. Nor will the ICO take any action over compliance with the fifth data protection principle or any equivalent under UK GDPR. It is, however, important to note that where data put beyond use is still held it might need to be provided in response to a court order.

22.21.4 The trust must work towards technical solutions to permanently delete data that has reached the end of its retention period, in particular during the early stages of procuring new electronic systems.

22.22 Email archiving

22.22.1 Email inboxes are not intended to be a filing system and records should only be held in line with the Records Management Code of Practice.

22.22.2 Emails should be retained if they constitute a business record or the attachment to the email retained as a record for a designated period of time.

22.22.3 In order to meet its legal and compliance needs, email servers will be backed up and archived.

22.23 Confidential waste disposal

22.23.1 KCHFT has in place an accredited confidential waste contractor.

22.23.2 All confidential, person identifiable and restricted material must be securely destroyed by shredding, or by using confidential waste collection facilities. When the latter is applicable, all confidential information must be stored securely prior to collection.

22.23.3 The confidential waste contract is managed KMPT Waste & Environment Team who can be contacted on 0300 303 3209 or via email kmpt.estatesandfacilitieshelpdesk@nhs.net

22.24 Data Quality

22.24.1 KCHFT has developed a Data Quality policy, which is available to view on Flo, with the aim of:

- communicating why good data quality is essential;

- outlining and raising the profile of data quality within KCHFT;
- ensuring that the basic principles of data quality are understood and implemented;
- outlining CQC Key Line of Enquiry S3, Data Security and Protection Toolkit data quality elements and introducing the information maturity assessment matrix tool;
- encouraging system leads to introduce change control processes for their systems, and;
- providing guidance in conducting an internal audit.

22.24.2 Data accuracy is the direct responsibility of the person inputting the data.

22.24.3 All systems include validation processes at input stage to check in full, or in part, the acceptability of the data. This validation may be used to maintain referential integrity.

22.24.4 Any loss or corruption of data should be reported to the relevant system manager immediately and recorded on Datix. If the incident involves a breach of the data protection legislation it may be considered a serious incident and must be reported to the Patient Safety team immediately.

22.24.5 For further information please view the Data Quality policy on Flo or if in any doubt about the quality of data within systems you use or questions regarding best practice contact the Performance team kcht.performanceteam@nhs.net who will be able to advise.

22.24.6 The Information Governance team have also launched a data quality awareness poster which is available on Flo, search ‘Take the time, every time’ poster. For further generic information regarding data quality issues which have resulted in breaches of data protection contact us on 0300 123 2079 or log a call on the IT Service Portal (click on Information Governance)

23.0 MONITORING COMPLIANCE AND EFFECTIVENESS OF THIS POLICY

23.1 Auditing and Monitoring Staff Compliance and Understanding

23.1.1 All IG learning and compliance will be monitored through either;

- Internal and external IG Service reviews and visual inspections
- Robust training programme
- Training completion
- Monitoring reduction in serious incidents and frequency and type of all other incidents.
- Policy dissemination process

23.2 Monitoring and Review

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

23.2.2 This policy will be continually monitored and will be subject to regular review by the IGAG. An earlier review may be warranted if one or more of the following occurs:

- As a result of regulatory / statutory changes or developments
- As a result of NHS policy changes or developments
- For any other relevant or compelling reason

23.2.3 Compliance with IG standards will be monitored regularly and in response to incidents and concerns. Compliance is the means by which KCHFT can gain assurance that policies and procedures are fully implemented and working well.

23.2.4 Compliance will be monitored and reported on through the IGAG. Where implementation or progress does not meet the high standards required, this will be considered for escalation and inclusion in the Annual Governance Statement and risk register.

23.2.5 Incidents and issues will be notified to the DPO, SIRO and CG, where patient/staff information is concerned.

23.2.6 Evidence supplied as part of the Data Security and Protection Toolkit (DSPT) is available to external organisations who may wish to inspect KCHFT documentation as part of audit. These organisations may include commissioners, the Care Quality Commission (CQC), the Information Commissioners Office (ICO) etc. and any other audit undertaken.

23.2.7 The DSPT informs the CQC registration requirements and evidence submitted will be used by the CQC to directly evidence their registration requirements.

24.0 EXCEPTIONS

24.1 None.

25.0 COMMUNICATION MATERIALS

Communications Channel	Purpose
Flo mail	• Weekly bulletin sent by email. • Suitable for factual articles and updates, directing people to new policies or significant changes to information on the intranet. • Articles should direct readers to sources of more detailed information rather than aim to convey it within the piece.
Global Email	• For emergencies only. • In the interest of the amount of email traffic in the organisation global emails can be sent but only for messages which genuinely can't wait for the next weekly bulletin.
Flo	• KCHFT staff intranet • Suitable for factual information, policies, procedures, documents and templates and any other information needed to support people in doing their jobs. • Suitable for updates or news stories which can be linked to other information pages on the site.

KCHFT website	- For information that you wish the public to see - For non-confidential information - Information should be factual and not contentious
Contract of Employment and Confidentiality Code of Conduct	To obtain agreement to adhere to policies and procedures
Staff Induction	Suitable for giving new staff a presentation and supporting information on IG
Staff Events	- Suitable for engaging with staff and raising awareness. - Particularly useful for staff who do not have regular internet access
Board Meeting Marketplace	Suitable for engaging with patients and public about issues.
Posters	- Suitable for drawing attention to issues affecting patients or raising awareness of new requirements among staff. - Public facing posters must be ratified by KCHFT Patient Information Group process.
Leaflets	- Suitable for drawing attention to issues affecting patients or raising awareness of new requirements among staff. - Public facing leaflets must be ratified by KCHFT Patient Information Group process.
Email Footer	For notifying Freedom of Information Lead and the contact for Subject Access Requests.
IG newsletter	Newsletter outlining all important messages for staff in bite-size form

26.0 GLOSSARY AND ABBREVIATIONS

Abbreviation	**Meaning**
Applicant	The individual(s), group or trust requesting access to information under the FOI Act or EIRs.
Caldicott Guardian	Director with a clinical background appointed to ensure anyone processing patient identifiable information within KCHFT applies the Caldicott seven general principles of good practice in handling such information (see under the Data Protection and Confidentiality Policy).
confidential	Confidential information includes, but is not limited to, all information of a confidential nature relating to the business and affairs of KCHFT, its' patients and employees, and any business or affairs of any other person to whom KCHFT has an obligation of confidentiality.
DPA98 / DPA18	Data Protection Act 1998/2018
Data	Information which is: - being processed by means of equipment operating automatically in response to instructions given for that purpose - recorded with the intention that it should be processed by means of such equipment - recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system
Data controller	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.

	NB: The data controller is usually KCHFT and not an individual in KCHFT
Data subject	An individual who is the subject of personal data
Duty to confirm or deny	Any person making a request for information to a public authority is entitled to be informed in writing by that public authority whether the public authority holds the information specified in the request or not.
European Economic Area	The member States of the European Union, together with Iceland, Liechtenstein, and Norway
EIR(s)	Environmental Information Regulations 2004
Exceptions	Applied to environmental information that is not appropriate to be made public. All EIR exceptions are "qualified" and therefore subject to the public interest test.
Fees notice	A written notification issued to an applicant stating that a fee is payable and exempts public authorities from being obliged to disclose information until the fee has been paid. The applicant will have three months from the date of notification to pay the fee before his/her request lapses.
Fees regulations	The regulations by which fees can be calculated in regard to the FOI Act. All local authorities have an appropriate limit of £450 for Prescribed costs under which no fee can be charged except for disbursements. The appropriate limit is calculated at £25 per person per hour per day to ascertain if the authority holds the information, then locating, retrieving and extracting.
FOI / The FOI Act 2000	Freedom of Information Act 2000
FOI Lead at Board Level	Delegated responsibility at director level or other equivalent standing for the Freedom of Information Act 2000 from the Chief Executive.
GDPR	General Data Protection Regulations
General right of access	Confers a general right of access to information held by public authorities; subject to exemptions (FOI Act) and exceptions (EIRs).
Health Record	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
Information Commissioner	Person appointed by Government to administer the provisions of the Data Protection Act and Freedom of Information Act. Before the FOIA, called the Data Protection Registrar (1984) or the Data Protection Commissioner (1998)
KCHFT / the trust	Kent Community Health NHS Foundation Trust
NHS organisations	All organisations providing health care services, including strategic health authorities, special health authorities, NHS trusts, general medical and dental practices
Password	Confidential authentication information composed of a string of characters numbers and symbols
Personal information / personal data	See "personal confidential data"
Personal confidential data	Data which relate to a living individual who can be identified: a) from that data

	b) from that and other information in the possession of, or likely to come in the possession of, the Data Controller c) includes 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
Processing (in relation to data)	Obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including: a) organisation, adaptation or alteration of the information or data b) retrieval, consultation or use of the information or data c) disclosure of the information or data by transmission, dissemination or otherwise making available alignment, combination, blocking, erasure or destruction of the information or data
Public authority	There are 100,000 public bodies and office holders listed under Schedule 1 ranging from Central Government departments to committees, the principle public authorities being: all government departments, the armed forces of the Crown, police, fire and ambulance services, the NHS, education authorities and local government.
Public Interest Test	The test to determine whether the public interest in withholding information under one of the qualified exemptions outweighs the public interest in releasing it.
Publication Scheme	Specifies the classes of information that a public authority publishes or intends to publish, the manner of publication and whether the information is available to the public free of charge or on receipt of payment.
Qualified exemption	Information to which a qualified exemption applies requires a public authority to take a test of prejudice or to demonstrate that the balance of public interest is in favour of non-disclosure. Reference to qualified exemptions can be found in Part I, section 2 and Part II of the FOI Act. Hyperlinks to each of the qualified exemptions are also provided in Appendix 1
Qualified Person	Is the Chief Executive of the trust and required to give their 'reasonable' opinion' that disclosure of information is exempt pursuant to Section 36 'prejudice to effective conduct of public affairs'. The trust must keep a record of the qualified person's opinion and the submission made to obtain that opinion. In the event of a complaint, the ICO will expect to see a record of the qualified person's opinion
Relevant filing system	Any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible
Special categories of personal data	Personal data consisting of information as to: • race or ethnic origin • political opinions • religious or philosophical beliefs • trade union membership • physical or mental health

	- sex life or sexual orientation - processing of genetic data, biometric data for the purpose of uniquely identifying a natural person [UK GDPR Article 9(1)]
UK GDPR	United Kingdom General Data Protection Regulations

27.0 CONTACTS

Information Governance	0300 123 2079	IT Service Portal (click Information Governance)
Archiving Service	0300 123 2079	IT Service Portal (click Information Governance)
Cyber and information systems	0300 123 1885	IT Service Desk from portal on desktop or ithelp.kentcht.nhs.uk
Data Protection Officer	**0300 123 2079**	kentchft.dataprotectionofficer@nhs.net
Caldicott Guardian	0300 123 2670	kcht.caldicottguardian@nhs.net
Senior Information Risk Owner	01622 211904	Gordon.flack@nhs.net
Legal Team	01233 667700	kcht.legal@nhs.net
Freedom of Information Lead	01622 211988	kcht.foi@nhs.net
IT Service Centre	0300 123 1885	IT Service Desk from portal on desktop or ithelp.kentcht.nhs.uk
Patient Safety Team	01233 667893	kentchft.patientsafetyteam@nhs.net

28.0 DATA PROTECTION IMPACT ASSESSMENT

28.1 Data Protection impact has been considered for this policy.

28.2 There are no privacy risks associated with it directly however, some of the processes which stem from it will have, and during the assessment of these processes or functions a Data Protection Impact Assessment may be deemed necessary.