Kent and Medway
NHS and Social Care Partnership Trust

Sharing Personal Information Policy

Document Reference No.	KMPT.InfG.062.08
Replacing document	KMPT.InfG.062.07
Target audience	Trust wide
Author	Information Governance and Records Management Department
Group responsible for developing document	Information Governance Group
Status	Authorised
Authorised/Ratified By	Information Governance Group
Authorised/Ratified On	May 2024
Date of Implementation	May 2024
Review Date	May 2025
Review	This document will be reviewed prior to review date if a legislative change or other event otherwise dictates.
Distribution date	June 2025
Number of Pages	16
Contact Point for Queries	kmpt.policies@nhs.net
Copyright	Kent and Medway NHS and Social Care Partnership Trust 2023

DOCUMENT TRACKING SHEET

Sharing Personal Information Policy

Version	Status	Date	Issued to/approved by	Comments
0.1	Draft	January 2017	ICT Benefits Realisation Manager	New policy combing Access to Personal Information Procedure, Information Rights Policy, Video and Audio Recording Procedure and the Patient's Right to Correspondence Policy
1.0	Approved	January 2017	Information Governance Group	Approved for use
1.1	Draft	May 2017	Information Governance Department	Reviewed, Updated and sent to IGG for approval
2.0	Approved	May 2017	Information Governance Group	Approved for use
2.1	Approved	November 2017	Information Governance Group	Separated Equality Impact Assessment from document.
2.2	Draft	May 2018	Information Governance Department	Reviewed updated and sent to IGG for approval
3.0	Approved	July 2018	Information Governance Group	Approved for use
3.1	Draft	March 2021	Information Governance Department	In year review update and issue for approval
4.0	Approved	March 2021	Information Governance Group	Approved for use
4.1	Draft	May 2022		Reviewed and updated and sent to IGG for approval.
5.0	Final	May 2022	Information Governance Group	Approved for use
5.1	Draft	March 2023		In year review
6.0	Final	May 2023	Information Governance Group	Approved for use
6.1	Draft	May 2024	Data Protection Officer	In year review – updated following audit
7.0	Final	May 2024	Information Governance Group	Approved for use
7.2	Draft	February 2025	IG&RM Security Lead	In year review
8.0	Final	February 2025	Information Governance Group	Approved

REFERENCES

Access to Health Records Act 1990
Access to Medical Reports Act 1988
ISO27001 Information Security Management
ISO9001 Quality Management
ISO14001 Environment Management
Caldicott Report 1997
Computer Misuse Act 1990
Confidentiality NHS Code of Practice 2003

Copyright, Designs and Patents Act 1988
Data Protection Act 2018
Electronic Communications Act 2000
Environmental Information Regulations 2004
Freedom of Information Act 2000
Fundamental Standards: Care Quality Commission
General Data Protection Regulation
Health and Social Care Act 2012
Human Rights Act 1998
Information Security Management: NHS Code of Practice
National Health Service Litigation Authority Standards
NHS Digital – Data Security and Protection Toolkit
NHSX Records Management Code of Practice October 2021

RELATED POLICIES/PROCEDURES/protocols/forms/leaflets

Data Protection and Confidentiality Policy	KMPT.InfG.071
Confidentiality Code of Conduct	KMPT.InfG.009
Data Quality Policy	KMPT.InfG.007
Email and Instant Messaging Acceptable Use Policy	KMPT.InfG.016
Overarching Information Governance Policy	KMPT.InfG.063
Information Governance Incident Management Policy and Procedures	KMPT.InfG.067
Information Systems Change and Accreditation Policy	KMPT.InfG.059
Internet Acceptable Use Procedure	KMPT.InfG.017
Health and Social Care Records Policy	KMPT.CliG.071
Management of Serious Incidents, Incidents, Accidents and Near Misses Policy	KMPT.CorG.017
Network Security Policy	KMPT.InfG.044
System Specific Security Policies	
Remote Working Policy	KMPT.InfG.041
Safe Haven Procedures	KMPT.InfG.015
Registration Authority Policy	KMPT.InfG.066
Sharing Personal Information Policy	KMPT.InfG.062

SUMMARY OF CHANGES

Date	Author	Page	Changes (brief summary)
July 2018	LM[c]		Policy updated to reflect changes in law following the introduction of the General Data Protection Regulation and UK Data Protection Act 2018
March 2021	AP		Updated records retention and destruction guidance to NHSX Records Management Code of Practice. Updated all references to Information Governance Department to include Records Management. Updated purpose to include audio, video and CCTV recordings Update made to Clinical Systems Team responsibilities.
May 2022	AP		In year review
March 2023	AP		In year review
March 2024	LMc	12-14	Updated to incorporate routine sharing and sharing agreements

CONTENTS

1 DOCUMENT SUMMARY

1.1 The Trust needs to collect and use information about people in order to carry out its business activities and fulfil statutory obligations. The information is held on past and current service users, employees, suppliers and others with whom we communicate.

1.2 Information takes many forms and includes data stored on computers, transmitted across networks, printed out, written on paper, sent by fax, stored on tapes and diskettes, or spoken in conversation and over the telephone.

1.3 Personal information must be handled properly, no matter how it is collected, recorded, used or disseminated. Legislation describes the obligations upon the Trust for information management, many of which extend to employees and agents of the Trust who may be held personally liable for any breaches.

1.4 To ensure the confidentiality of information the Trust must safeguard its records and record keeping systems to protect against unauthorised disclosure, modification or interruption. Information sharing must, at all times, be done in a lawful, ethical and effective manner to ensure that all legislation, regulation, best practice and guidance are adhered to at all times.

1.5 The Trust's Information Governance Policies set out the minimum policy standards for the handling of information. They cover the overlapping areas of data protection compliance, information security, data quality, freedom of information and confidentiality.

1.6 This policy describes how staff must manage information which identifies an individual. It provides detailed guidance for responding to requests for information received under different circumstances and made by different requesters. This policy covers the sharing of both staff and patient personal information.

2 INTRODUCTION

2.1 The Trust encourages the lawful and appropriate sharing of information, both for patient care and service management as determined by law, statue and best practice, whilst recognising and respecting a patient's right to confidentiality. This Policy is a guide for staff for responding to the different types of requests which may be received for access to personal information of both staff and patients.

2.2 In addition to various legislative requirements the Government's commitment to implement the recommendations of the Caldicott Committee requires the Trust to have a Caldicott Guardian to ensure the protection and use of confidential information. This Policy provides guidance on the Caldicott Principles and role of the Caldicott Guardian.

2.3 This Policy also describes a Department of Health initiative that expects clinicians to systematically give patients a copy of all correspondence between clinicians about them.

3 PURPOSE

3.1 The General Data Protection Regulation, and UK Data Protection Act 2018 enables individuals to access records, or be provided with photocopies, of the personal information held about them under the Act and, in the case of deceased individuals, under the Access to Health Records Act 1990. Such access could include but is not limited to all information stored within email accounts, network drives, medical records, employee records, minutes of meetings, documented discussions, audio and video recordings, including CCTV.

3.2 Information sharing must, at all times, be completed in a lawful, ethical and effective manner to ensure that all legislation, regulation, best practice and guidance are adhered to at all times. The objectives of this policy are to describe to all staff:

3.2.1 The legal framework governing confidentiality and the use and disclosure of personal information

3.2.2 Their individual responsibilities for compliance with the law and best practice

3.2.3 The information that is considered confidential

3.2.4 The circumstances under which personal information held within the Trust can be disclosed

3.2.5 Who to approach within the Trust for assistance with disclosure issues

3.2.6 Possible sanctions for breach of confidentiality and legislation

3.2.7 The guidance for recording video and audio during patient sessions for sharing with the patient or for research purposes

3.2.8 The requirement to systematically disclosure to patients copies of all correspondence between clinicians about them.

4 DUTIES

4.1 Caldicott Guardian

4.1.1 The Caldicott Guardian is responsible for agreeing, monitoring, and reviewing protocols governing the use of personally-identifiable information, both within the Trust and across organisations, e.g. with other NHS and local authority services, and other partner organisations contributing to the local provision of care, in compliance with UK legislation and national policy and guidance.

4.2 Data Protection Officer (DPO)

4.2.1 The Data Protection Officer is the Head of Information Governance and Records Management. The Data Protection Officer has overall responsibility for managing and effectively implementing all activities necessary to achieve compliance with the GDPR and UK DPA 18 throughout the Trust:

- To inform and advise the organisation and its employees about their obligations
- To comply with the GDPR and other data protection laws
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (patients/staff)

4.3 Senior Information Risk Owner (SIRO)

4.3.1 The Senior Information Risk Owner (SIRO) and has executive responsibility for the identification, definition and implementation of an information security risk programme. The SIRO chairs the Information Governance Group.

4.4 Information Governance Group

4.4.1 The Information Governance Group is responsible for information governance compliance and is therefore required to review policies, procedures, training and awareness and ensure resources are available to implement them. The Information Governance Group oversees the work of the Information Governance and Records Management Department to ensure that the Trust can meet the legal requirements and best practice responsibility for sharing personal information.

4.5 Information Governance and Records Management Department

4.5.1 The Information Governance and Records Management Department is responsible for the operational compliance of this policy, specifically managing all requests to access personal information.

4.5.2 The Information Governance and Records Management Department support the delivery of the Data Protection agenda and ensure service users are provided with information on their rights under the legislation, which includes deadline with subject access requests.

4.5.3 The Information Governance and Records Management Department support the Caldicott Guardian to deliver the Caldicott function. They conduct investigations into complaints about breaches of confidentiality, monitor compliance with the General Data Protection Regulation and UK Data Protection Act 2018 and the effectiveness of procedures through the use of system audits and ensure that appropriate action is taken where non-compliance is identified.

4.5.4 The Information Governance and Records Management Team are responsible for records management across the Trust, specifically the development of the Records Management policies, procedures and training material.

4.6 Clinical Information Systems Team

4.6.1 Registration Authority Agents are responsible for ensuring RA services are delivered to staff in accordance with RA policy; including registration of sponsors and healthcare professionals in the Trust, to ensure appropriate access controls are in place for personal information stored on computer.

The Clinical Systems Team are responsible for the overall management of multiple clinical information systems, ensuring all systems are managed to provide optimal support and function across the Trust.

4.7 Human Resources Directorate

4.7.1 The HR Directorate is responsible for overseeing the policies and procedures to creating, maintaining and using staff personnel files. The Directorate is responsible for ensuring all staff sign confidentiality (non-disclosure) undertakings as part of their contract of employment and is responsible for ensuring information governance responsibilities are detailed in all job descriptions and staff contracts for employment.

4.8 Line Managers

4.8.1 Line Managers are responsible for data protection practice within their work area by ensuring all that their staff have completed the Information Governance eLearning Training programme, and that their Team work in accordance with the Trust's Information Governance policies. Managers must ensure that their staff receive all Information Governance briefings to ensure they remain adequately trained and aware of their personal responsibilities for data protection, Caldicott and RA issues.

4.9 Staff Responsibilities

4.9.1 All staff are responsible for reading and complying with Trust policy and guidance, and completing all mandatory training. Each employed, contracted and voluntary staff member is personally responsible for ensuring that no breaches of confidentiality result from their actions or inactions.

5 GENERAL DATA PROTECTION REGULATION AND DATA PROTECTION ACT 2018

5.1 The General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA) regulates the processing of personal data. Personal data means data which relates to an identified or identifiable living individual. Under the Act, Sensitive personal data or special category data requires additional controls to protect it while processing. Information relating to the health of an individual is classified as sensitive personal data, or special category data.

5.2 Processing in relation to information or data, means collating, recording or holding the information or carrying out any operation or set of operations on the information, including disclosure. Processing includes both automated and unautomated actions. This policy is concerned with the correct processes staff must follow when sharing the personal data of both staff and service users.

5.3 The Information Governance and Records Management Department is operationally responsible for compliance with the GDPR / DPA 18 and the Caldicott Guardian is the nominated person with responsibility for the internal protocols governing access to personal information. These individuals will take the lead on ensuring all staff managing and handling personal information are aware of their responsibilities and that all enquiries about personal information are handled appropriately and dealt with according to Trust procedures.

5.4 It is an offence under section 170 (1) of the Data Protection Act 2018 to unlawfully obtain, disclose, or retain personal data without the consent of the data controller

6 ACCESS TO HEALTH RECORDS ACT 1990

6.1 The ethical obligation to respect a patient's confidentiality extends beyond death. However, this duty of confidentiality needs to be balanced with other considerations, such as the interests of justice and of people close to the deceased person. Statutory rights of access to the data of deceased patients are set out in the Access to Health Records Act 1990.

6.2 Unless a patient requested confidentiality while alive, their personal representative and any other person who may have a claim arising out of the patient's death has a right of access to information in the deceased person's records directly relevant to a claim.

6.3 Under the terms of the Act, requesters will only be able to access the deceased's health records if they are either:

6.3.1 A personal representative (the executor or administrator of the deceased person's estate)

6.3.2 Someone who has a claim resulting from the death (this could be a relative or another person)

6.4 The Information Governance and Records Management Department are operationally responsible for compliance with the Access to Health Records Act.

7 CALDICOTT

7.1 The original six general principles for information governance were published in 1997, following the Caldicott Review. They describe acceptable use for all organisations with access to patient information. A review of those 6 principles in 2013 noted an additional principle and redefined them as:

7.1.1 **Justify the purpose(s)**

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

7.1.2 **Don't use personal confidential data unless it is absolutely necessary**

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

7.1.3 **Use the minimum necessary personal confidential data**

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

7.1.4 **Access to personal confidential data should be on a strict need-to-know basis**

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

7.1.5 **Everyone with access to personal confidential data should be aware of their responsibilities**

Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

7.1.6 **Comply with the law**

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7.1.7 **The duty to share information can be as important as the duty to protect patient confidentiality.**

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

7.2 The Trust's Caldicott Guardian, supported by the Information Governance and Records Management Department, ensure that the Trust complies with these principles in the processing of patient information, and that staff are trained to consider them whenever processing personal data.

8 SHARING CLINICAL INFORMATION

8.1 Service users are entitled to expect that their personal information will remain confidential. They must feel able to discuss sensitive matters without fear that the information may be improperly disclosed. The Health Service cannot work effectively without trust and trust depends on confidentiality. However, people also expect professionals to share information with other members of the care team, who need to co-operate to provide a seamless, integrated service. Therefore, good sharing of information, when sharing is appropriate, is as important as maintaining confidentiality. The Trust must succeed in both respects if we are not to fail the people that we exist to serve.

8.2 In line with the General Data Protection Regulation / Data Protection Act 2018 clinical teams are able to share relevant and necessary information with other health and social care professionals for the provision of health or social care treatment without the requirement to obtain consent from service users.

8.3 Where Information is being shared for purposes other than the provision of health or social care treatment, it will be necessary to relay on an alternative legal basis for sharing, such as service user consent.

8.4 INFORMAL ACCESS REQUESTS

8.4.1 Informal disclosure of personal information can occur where an individual is currently receiving treatment or care from the Trust.

8.4.2 A patient of the Trust who is currently being treated by a Service can approach their Care Co-ordinator or Consultant for an informal viewing of their health records.

8.4.3 The Care Co-ordinator or Consultant must record, in the health record, where informal disclosure has been either made or denied.

8.4.4 Informal disclosure only involves showing the individual the information and explaining its meaning and purpose. It does not extend to requests for copies from the record. Where an individual requests copies of any of the information recorded in the file, the process for formal access must be followed.

8.4.5 Informal disclosure only extends to a request from the individual. Requests from relatives or representatives of the individual must be considered as a formal request and treated in accordance with Section 8.5 below.

8.4.6 Informal disclosures can occur except in the following circumstances: -

- Where the information is likely to cause serious harm to the physical or mental health of the individual or another individual; and
- Where the information could identify a third party (unless the third party in question has specifically consented to the disclosure, in writing).
- Where a patient is denied informal access, they should be advised of their right to make a formal application, but be advised that there is no guarantee of disclosure.
- Where the request comes from a patient who has been discharged from the Service, the request will need to be made via a formal application.

8.5 FORMAL ACCESS REQUESTS

8.5.1 A formal request for access to personal information can be made by any individual who has either had contact with the Trust or has the consent of the individual who has had contact with the Trust.

8.5.2 Such requests may be received verbally or in writing and be for either a full copy of everything held, or specific time-periods/documents.

8.5.3 All enquiries for formal access to personal information must be immediately passed to the Information Governance and Records Management Department based at Farm Villa, Maidstone.

8.5.4 The Information Governance and Records Management Department follow their standardised procedures for handling and processing a request within the timescales stipulated in the appropriate legislation (currently one calendar month for requests under the Data Protection Act 18 and 21 or 40 calendar days for requests under the Access to Health Records Act dependant on the individual request).

8.5.5 All formal access requests require a clinical review prior to release of the records and this must be completed by a "registered Health or Social Care professional" as stipulated within the legislation.

8.5.6 The clinical review process is to ensure that

- The information will not cause serious harm to the physical or mental health of the individual or another individual; and
- The information does not identify a third party (unless the third party in question has specifically consented to the disclosure, in writing).

8.5.7 Trust staff will be required to assist the Information Governance and Records Management Team during the process in respect of locating and retrieving records and reviewing information prior to release.

8.6 CONTINUING CARE REQUESTS – OTHER NHS TRUSTS

8.6.1 If a request for information is made from another NHS organisation and is required for a purpose directly related to the provision of care, summary information can be provided without the explicit consent of the service user.

8.6.2 The Trust is required to adequately satisfy itself of the identity of the requestor i.e. through a request in writing on NHS letterhead or other means. Requests of this type, unless urgent, should be forwarded to the Information Access Team kmpt.infoaccess@nhs.net

8.6.3 The Information Governance and Records Management Department will provide a photocopy of the latest discharge summary and/or care plan and risk documentation as relevant to the requesting NHS organisation. If the NHS Trust requires the information for purposes other than to continue care or require a full copy of the records, the consent of the service user may be required and the request sent through to the Information Governance and Records Management Department.

8.6.4 Original records **must** at all times remain in the possession of the Kent and Medway Health and Social Care Partnership Trust.

8.6.5 All disclosures must be transmitted securely in accordance with the Trust's Safe Haven Policy.

8.7 AUDIT/RESEARCH REQUESTS

8.7.1 Individuals undertaking audit and/or research activities must ensure their work is approved by the Trust's Research and Development Team prior to being provided with access to personal information.

8.8 NON NHS WORK

8.8.1 Consultants wishing to have access to case notes for use in private consultation must adhere to the procedures for making a formal access request to view the record (see Section 8.5 above).

8.8.2 Signed consent or evidence of request to complete private work must be obtained from the individual and submitted to the Information Governance and Records Management Department with a written request.

8.9 COPYING CORRESPONDENCE TO PATIENTS

8.9.1 All clinicians must copy to patients, any correspondence between clinicians about them, unless either or both of the following Data Protection Act 2018 exceptions apply, or with documented agreed with the patient:

a) The document (letter, report etc.), either contains information likely to harm the patient or another individual; or

b) The document contains confidential information about a third party.

8.9.2 If clinicians have any doubt as to the potential impact of the content of a letter on the patient's mental health, they are advised to err on the side of caution and not copy the letter so as to prevent harm.

8.9.3 In doing so, they may wish to discuss the matter with a colleague who knows the patient before forming an opinion as to the extent of the likely harm.

8.9.4 Clinicians must check with their patients at the beginning of their involvement:

- If they wish to get a copy of every letter, if they would prefer a copy of the discharge summary instead, or if they do not want to receive any letter at all; and
- If they have a preference in how they wish to receive correspondence such as via email or via post (to avoid sending confidential information to the wrong address).
- All correspondence sent to patients must be marked "private and confidential" (but does not have to be sent in registered delivery) and have a return address on the envelope.

9 SHARING PERSONNEL INFORMATION

9.1 The Data Protection Act 2018 provides the same rights of access for staff information held by the Trust as it does for service user data.

9.2 INFORMAL ACCESS REQUESTS

9.2.1 Informal disclosure of personal information can occur where an individual is currently employed by the Trust.

9.2.2 An employee can, at any time, approach their Line Manager for an informal viewing of their personal file. Such informal disclosure is not considered to be a formal application and, in many cases, may avoid the necessity for such formal applications.

9.2.3 The Line Manager should record, in the file, where informal disclosure has been either made or denied.

9.3 FORMAL ACCESS REQUESTS

9.3.1 A formal request for access to personal information can be made by any individual or organisation who has either had contact with the Trust or has the consent of the individual who has had contact with the Trust.

9.3.2 Such requests may be received verbally or in writing and be for either a full copy of everything held, or specific time-periods/documents.

9.3.3 All enquiries for formal access to personal information must be immediately passed to the Information Governance and Records Management Department based at St Michaels House, Sittingbourne.

9.3.4 The Information Governance and Records Management Department will carry out local procedures for handling and processing a request within the timescales stipulated in the appropriate legislation (currently one calendar month for requests under the Data Protection Act 18 and 21 or 40 calendar days for requests under the Access to Health Records Act dependant on the individual request).

9.3.5 Trust staff will be required to assist the Information Governance and Records Management Department during the process in respect of locating and retrieving records and reviewing information prior to release.

10 OTHER ENQUIRIES

10.1 Trust staff may receive other enquiries from external agencies and/or third parties requesting the sharing of confidential or personal information about an employee or service user.

10.2 Any such request should be considered on a case by case basis and information disclosed only where to do so would not breach any of the Data Protection Principles or Caldicott Guidelines.

10.3 Advice and guidance should be obtained from the Information Governance and Records Management Department

10.4 Where an enquiry relates to safeguarding of Adults or Children, advice and guidance should be obtained from the Safeguarding Team as well as the Information Governance and Records Management Department.

10.5 Any disclosure must be relevant and proportionate to the request received and take into consideration any safeguarding or clinical risk. The decision to disclose must be supported by either a Senior Clinician, Care Co-ordinator or Line Manager of the individual and be fully documented within the records held by the Trust including what was disclosed, who to and, where released without consent, the justification for doing so.

10.6 All disclosures must be transmitted securely in accordance with the Safe Haven Policy.

11 AUDIO AND VIDEO RECORDING OF PATIENT SESSIONS

11.1 This section of the policy provides guidance to clinicians on the retention of video and audio recordings of clinical interactions which are an aid to therapy, clinical training or supervision and do not form part of the clients/patient's clinical record.

11.2 A recording is considered to be an aid to therapy where it is undertaken not to produce a clinical record but to support the patient in their therapeutic journey. The data is only retained as agreed with the patient and then securely destroyed.

11.3 RECORDING AS AN AID TO THERAPY

11.3.1 Before any recording (either video or audio) takes place, explicit consent must be obtained from the patient and recorded in the Information Sharing and Consent Form on Rio. Discussions about consent should include:

- the method of recording, either video or audio etc.
- that the recording will not form part of the clinical record; and
- that, if the recording is retained by the Trust, the recording will be destroyed after use, within the time span agreed with the patient. If the recording is to be given to the patient, then the responsibility for retention and destruction transfers to the patient.

11.3.2 Where the patient is deemed without capacity to consent, a multi-disciplinary case conference with the patient's nearest relative should decide in relation to "best interest" and "duty of care".

11.3.3 Where it is agreed that the recording will be retained by the patient, the responsibility for secure retention and disposal transfers to the patient at the point at which the Trust provides the recording. An entry must be made in the patient's clinical record noting the transfer of the recording to the patient.

11.3.4 Where it is agreed with the patient that the Trust will retain the recording, it must be held securely and destroyed securely at the agreed time, in accordance with the Trusts policy on disposal of confidential waste. An entry must be made in the patient's clinical record noting the type and date of recording and date and method of destruction.

11.4 RECORDING FOR PURPOSES OF CLINICAL SUPERVISION OR TRAINING/PRESENTATION TO EXAMINING BODIES

11.4.1 Where it is proposed that a recording is to be retained for training purposes, presentation to examining bodies or writing of case studies, separate and explicit written permission must be obtained from the patient. The consent should include the same information as detailed in 11.3.1 above.

11.4.2 Any information used for training or presentation as part of a case study must be anonymised. Therefore, care must be taken to remove any personal identifiers that are not clinically required.

11.4.3 There is no prescribed time limit for holding the recording however, as part of obtaining consent from the client, an indicative time period will have been provided. In any event, a regular review of the benefits of retaining the recording should be undertaken (at least every six months). Where the recording is no longer required it must be destroyed in accordance with the Trust's Information Security Policy on the disposal of confidential waste and an entry made in the patient's clinical notes identifying the type and date of the recording and date and method of destruction.

11.4.4 Where the client is deemed without capacity to consent to the recording for the purpose of training or supervision, the same procedures as indicated in 11.3.2 above should be undertaken.

11.5 RECORDING AND TRANSCRIPTION

11.5.1 It may be considered appropriate to use a dictating machine to record the information for later transcription. Staff are only permitted to use Trust issued dictation equipment. Once transcribed, the recording must be securely destroyed.

11.5.2 Where the recording is retained for the purposes of case studies or presenting to an examining body, it is recognised that the retention period may be longer. Recordings

must be stored safely and retained in a secure location on Trust premises; and if removable media is used, this must be Trust issued i.e. encrypted memory stick.

12 AUDIO AND VIDEO RECORDING UNDERTAKEN BY A SERVICE USER

12.1 Overt patient recordings

12.1.1 Although we cannot place restrictions on a patient wishing to record notes of a consultation or conversation with a health professional, where it is felt absolutely necessary by the patient to do so, we should ensure that:

- any recording is done openly and honestly
- the recording process itself does not interfere with the consultation process or the treatment or care being administered
- the patient understands that a note will be made in their health record stating that they have recorded the consultation or care being provided
- the patient is reminded of the private and confidential nature of the recording and that it is their responsibility to keep it safe and secure
- any recording is only made for personal use
- patients are aware that the misuse of a recording may result in criminal or civil proceedings
- patients are discouraged from undertaking recordings in the first place, unless it is deemed absolutely necessary by highlighting the above responsibilities.

12.2 Covert patient recordings

12.2.1 Although we cannot place restrictions on a patient wishing to covertly record a consultation or conversation with a health professional, where organisations are aware that covert recording is a significant issue they should aim to discourage patients from doing so by ensuring that:

- the organisation promotes the open and honest recording of consultations, where a patient deems it absolutely necessary (see the advice above, which applies equally to covert recording)
- patients are aware that the organisation takes proactive steps to investigate and address any issues regarding the patient's treatment and care, to avoid them feeling it necessary to record their consultation
- relevant staff should consider providing patients with a written record summary, and or a verbatim record (if practical) of their consultation for their own personal use
- patients are advised that they are entitled to see their notes, if they so wish, by informally asking the healthcare professional in charge of the consultation, or to request a copy of their medical notes formally through a Subject Access Request (SAR) made under the Data Protection Act 2018
- patients are given information on how they can complain if they have an issue with their treatment and care, and their attention is drawn to the relevant guidance from the Care Quality Commission and Information Commissioner's Office.

13 ROUTINE, EXCEPTIONAL AND ON-OFF DICLOSURES OF INFORMATION WITH OTHER ORGANISATIONS

13.1 Sharing of non-personal information

13.1.1 Some information sharing does not involve personal data, for example where only statistics that cannot identify anyone are being shared.

13.1.2 Anonymous or aggregate (numbers) information may be shared internally or with other organisations for example to: improve patient experience; facilitate commissioning of services; manage and plan future services; facilitate quality improvement and clinical leadership; assure and improve the quality of care and treatment; statutory returns and requests; train staff; audit performance.

13.1.3 Refer to the ICO anonymisation code of practice for further information.

13.2 Sharing personal information with other organisations

13.2.1 Necessary and proportionate, personal information may be shared with other organisations for example to: investigate complaints or potential legal claims; protect children and adults at risk; assess need, service delivery and treatment.

13.2.2 This policy covers two main types of information sharing:

- 'Systematic' information sharing. This will generally involve routine sharing of data sets between organisations for an agreed purpose. It could also involve a group of organisations arranging to 'pool' their data for specific purposes.
- Exceptional or 'one-off' information sharing. Much information sharing takes place in a pre-planned and routine way. As such, this should be governed by established rules and procedures. However, departments/staff may also decide, or be asked, to share information in situations which are not covered by any routine agreement. In some cases, this may involve a decision about sharing being made in conditions of real urgency, for example in an emergency situation. All ad-hoc or one off sharing decisions must be carefully considered and documented.

13.2.3 **Factors to consider.** When deciding whether to enter into an arrangement to share personal data (either as a provider, a recipient or both) you should consider what is the sharing meant to achieve? There should be a clear objective or set of objectives. Being clear about this will identify the following:

- **Could the objective be achieved without sharing the data or by anonymising it?** It is not appropriate to use personal data to plan service provision, for example, where this could be done with information that does not amount to personal data.
- **What information needs to be shared?** You should not share all the personal data you hold about someone if only certain data items are needed to achieve the objectives. The third Caldicott principle specifies "Use the minimum necessary personal confidential data ".
- **Who requires access to the shared personal data?** You should employ 'need to know' principles, meaning that when sharing both internally between departments and externally with other organisations, individuals should only have access to your data if they need it to do their job, and that only relevant staff should have access to the data. This should also address any necessary restrictions on onward sharing of data with third parties.
- **When should it be shared?** It is good practice to document this, for example setting out whether the sharing should be an on-going, routine process or whether it should only take place in response to particular events.
- **How should it be shared?** This involves addressing the security surrounding the transmission or accessing of the data and establishing common rules for its security.

- **How can we check the sharing is achieving its objectives?** You will need to judge whether it is still appropriate and confirm that the safeguards still match the risks.
- **How are individuals made aware of the information sharing?** Have individuals been provided with the fair processing information as required by the GDPR? How is it ensured that individual's rights are respected and can be exercised e.g. how can they access the information held once shared?
- **What risk to the individual and/or the organisation does the data sharing pose?** For example, is any individual likely to be damaged by it? Is any individual likely to object? Might it undermine individuals' trust in the organisations that keep records about them?
- **Is the information subject to the National Data Opt-out Programme?** If a patient has exercised their rights under this programme, care must be taken not to share that data.
- **What is the legal basis for data protection purposes?** Organisations must identify the lawful basis (e.g. meeting statutory duties) for processing and, where necessary, a condition for processing special categories data (e.g. managing a health and care service).
- **If the information is confidential, what is the legal basis that complies with the common law duty of confidence?** This can be consent (implied or explicit), overriding public interest or required or permitted by law.

It is good practice to document all decisions and reasoning related to the information sharing.

13.2.4 In all circumstances of information sharing, staff will ensure that:

- When information needs to be shared, sharing complies with the law, guidance, best practice is followed and an information sharing agreement is in place;
- Only the minimum information necessary for the purpose will be shared;
- Individuals' rights will be respected, particularly confidentiality, security and the rights established by the GDPR;
- Confidentiality must be adhered to unless there is a robust public interest or a legal justification in disclosure;
- Reviews of information sharing should be undertaken to ensure the information sharing is meeting the required objectives/purpose and is still fulfilling its obligations

14 INFORMATION SHARING AGREEMENTS

14.1 Information sharing agreements, set out a common set of rules to be adopted by the various organisations involved in an information sharing operation. These could well form part of a contract between organisations. It is good practice to have an information sharing agreement in place, and to review it regularly, particularly where information is to be shared on a large scale, or on a regular basis.

14.2 An information sharing agreement must, at least, document the following:

- the purpose, or purposes, of the sharing;
- the legal basis for sharing under the DPA2018/GDPR;
- the legal basis to comply with the common law duty of confidence;
- the potential recipients or types of recipient and the circumstances in which they will have access;
- who the data controller(s) is and any data processor(s)
- the data to be shared;

- data quality – accuracy, relevance, usability;
- data security;
- retention of shared data;
- individuals' rights – procedures for dealing with access requests, other applicable GDPR rights, queries and complaints;
- review of effectiveness/termination of the sharing agreement; and
- any particular obligations on all parties to the agreement, giving an assurance around the standards expected sanctions for failure to comply with the agreement or breaches by individual staff

14.3 An information sharing agreement should be used when KMPT, acting as data controller, is sharing information directly with other organisations that will act either as a joint data controller with, or as data controllers in their own right for that information.

14.4 Any processing by an organisation on behalf of KMPT shall be governed by a data processing agreement, not an information sharing agreement. The GDPR requires a contract, or other legal act that is binding on the processor with regard to KMPT as data controller, that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

15 IMPLEMENTATION INCLUDING TRAINING AND AWARENESS

15.1 Training and awareness material for Information Governance initiatives is developed and implemented under the supervision of the Trust Information Governance Group. All staff must complete e-Leaning packages on Data Security Awareness as part of their induction and on a regular basis for refresher training.

15.2 Information Governance updates will be regularly supplied to staff through the Trust's Intranet, Technology News and staff briefings.

16 STAKEHOLDER INVOLVEMENT AND CONSULTATION

16.1 This policy has been developed in consultation with;

16.1.1 Director of Digital Services

16.1.2 Caldicott Guardian

16.1.3 Senior Information Risk Owner

16.1.4 Deputy Head of Clinical Systems

16.1.5 Information Governance and Records Management Department

16.1.6 Digital Services Service Managers

16.1.7 System Managers

16.2 This policy was reviewed and approved by the Trust-wide Information Governance Group.

17 EQUALITY IMPACT ASSESSMENT

17.1 The Equality Act 2010 places a statutory duty on public bodies to have due regard in the exercise of their functions. The duty also requires public bodies to consider how the decisions they make, and the services they deliver, affect people who share equality protected characteristics and

those who do not. In KMPT the culture of Equality Impact Assessment will be pursued in order to provide assurance that the Trust has carefully considered any potential negative outcomes that can occur before implementation. The Trust will monitor the implementation of the various functions/policies and refresh them in a timely manner in order to incorporate any positive changes.

18 HUMAN RIGHTS

18.1 The Human Rights Act 1998 sets out fundamental provisions with respect to the protection of individual human rights. These include maintaining dignity, ensuring confidentiality and protecting individuals from abuse of various kinds. Employees and volunteers of the Trust must ensure that the trust does not breach the human rights of any individual the trust comes into contact with. If you think your policy/strategy could potentially breach the right of an individual contact the legal team.

19 MONITORING COMPLIANCE WITH AND EFFECTIVENESS OF THIS DOCUMENT

19.1 The Trust is required to evidence it's adherence to Information Rights through the completion of the annual Information Governance Toolkit. It is also answerable to the Information Commissioner in respect of compliance with the Data Protection Act 1998.

19.2 The table below sets out the minimum requirements for monitoring under the requirements of this Policy.

What will be monitored	How will it be monitored	Who will monitor	Frequency	Evidence to demonstrate monitoring	Action to be taken in event of non compliance
Compliance with Section 45 of DPA	Reports to Information Rights Department and IG Group showing statistics and performance	Information Governance and Records Management Department	Monthly and Bi-monthly	Reports	Review of Services provided and performance management
Staff awareness of Procedures	Random surveys to Trust sites	Information Governance and Records Management Department	Annually	Report of Results to IG Group	Caldicott Incident log and increase staff awareness of requirements
Patient awareness of Confidentiality and Trust procedures	Patient Satisfaction Survey	Information Governance and Records Management Department	Annually	Application for Survey, Questionnaire and Clinical Audit assistance, Report of results from Survey	Increase awareness of staff requirements to pass down to patients to ensure better understanding
Access to patient information systems by authorised staff	Random and regular audits of information accessed by staff with Smartcards	Information Governance and Records Management Department	Monthly	Internal Caldicott procedures detailing audit requirements and inclusion in the Caldicott report to the IG Group	Investigation into any inappropriate use as required by RA Procedures and Information Security procedures

20 EXCEPTIONS

20.1 There are no exceptions to this policy.