Policy:

IMST 010 - Recording Policy

Executive Director Lead	Executive Director of Finance & SIRO
Policy Owner	Data Protection Officer
Policy Author	Data Protection Officer

Document Type	Policy
Document Version Number	v1.3
Date of Approval By PGG	30.01.2023
Date of Ratification	18/04/2023
Ratified By	ARC
Date of Issue	
Date for Review	01/2026

Summary of policy
This policy governs the use of audio and video recordings within the Trust by staff, volunteers, service users and carers.

Target audience	SHSC staff, volunteers, service users and carers

Keywords	Audio, video, recording, surveillance

Storage & Version Control

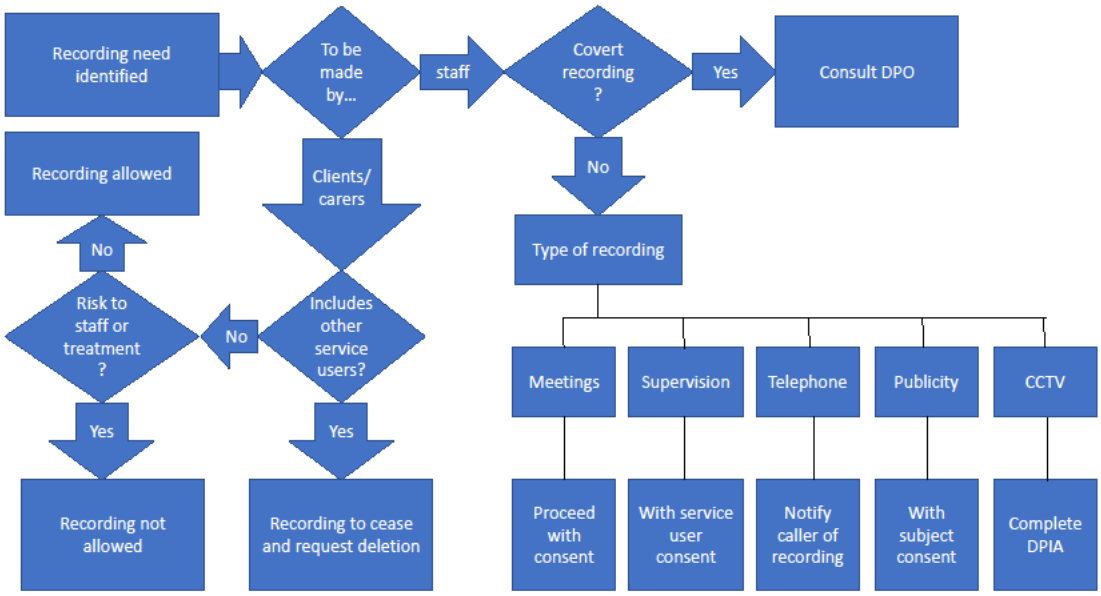
Version 1.3 of this policy is stored and available through the SHSC intranet/internet.. This version of the policy supersedes the previous version (1.2 02/2020). Any copies of the previous policy held separately should be destroyed and replaced with this version.

Version Control and Amendment Log

Version No.	Type of Change	Date	Description of change(s)
1	Draft policy created	02/2019	New policy commissioned on approval of a Case for Need
1.1	Draft policy amended	07/2019	Amended in light of comments
1.2	Draft policy amended	12/2019	Further amendments and formatting. Addition of section or recording meetings.
1.2	Approved by Data & Information Governance Board	01/2020	
1.3	Complementary Policy development	12/2022	Data & Information Governance Group notified of a new CCTV/Surveillance Camera (Inpatient Areas) Policy commissioned by the Least Restrictive Practice Group which replaces the previously agreed CCTV appendix to the Recording Policy.
1.4	Revised and updated	01/2023	Minor updates to reflect organisational change, new policies and national guidance.

Contents

Flowchart


Recording need identified
To be made by...
staff
Covert recording ?
Yes
Consult DPO
No
Type of recording
Clients/ carers
Recording allowed
No
Risk to staff or treatment ?
No
Includes other service users?
Yes
Yes
Recording not allowed
Recording to cease and request deletion
Meetings
Supervision
Telephone
Publicity
CCTV
Proceed with consent
With service user consent
Notify caller of recording
With subject consent
Complete DPIA

1 Introduction

As the capability to make audio and video recordings becomes cheaper and more widespread there have been more instances of service users, carers and staff making electronic recordings. This policy sets out principles to control such recordings to ensure that they meet national guidance and legal requirements.

2 Scope

This policy applies to all Trust staff, volunteers, service users, carers and others involved with Trust business.

3 Purpose

This policy regulates the use of audio and video recordings within the Trust. A separate policy provides more detailed guidance on Surveillance cameras/CCTV.

4 Definitions

Covert recordings: Audio or video recordings made without the knowledge of the people being recorded.

Data Protection Impact Assessment (DPIA): An assessment made before any significant new processing of person-identifiable information or change to existing processing to ensure it complies with data protection regulations and to identify any risks the processing presents. A template for DPIAs is available from the Data Protection Officer.

Skype: Skype is a proprietary telecommunications application which can be used for both voice and video communication.

Microsoft Teams: a proprietary business communication platform which includes workspace chat and videoconferencing, file storage, and application integration.

Surveillance Cameras: Video cameras used to monitor areas within the Trust including wards, corridors, server rooms, car parks or other places used by staff, service users, visitors or members of the public. Surveillance cameras may be used for live video or the images may be recorded. Surveillance cameras include cameras mounted in fixed positions and cameras worn or carried by members of staff.

5 Detail of the policy

This policy provides an overview of how audio and video recordings are managed within the Trust.

6 Duties

Role		Responsibility	Description
Chief Digital Information Officer	CDIO	Director, SHSC Digital	Responsible for the Information Technology that supports the overarching strategies of the Trust

Senior Information Risk Owner	SIRO	Executive Director Finance	Owns the Trust's information risk policy and risk assessment process
Caldicott Guardian	CG	Executive Director Medical	Responsible for protecting the confidentiality of patient and service user information and enabling the appropriate level of information sharing
Information Governance Manager			Responsible for the application of Information Governance throughout the Trust and compliance with the Data Security & Protection Toolkit,
Data Protection Officer	DPO		Supporting Trust wide Data & Information governance in accordance with UKGDPR, NHS Digital & England and Data Security & Protection Toolkit.
Information Asset Owners	IAO	Directorate	Senior representatives of the directorates closely aligned to major stores of organisational data, information and systems
Information Asset Managers	IAM	Service Managers	Primary administrative and management responsibilities for segments of data primarily associated with their functional area
All SHSC Staff and Volunteers			Responsible for compliance with Trust policy and reporting of any incidents

7 Procedure

7.1 Covert Recordings by Staff

The Trust does not usually authorise or undertake covert recordings, whether audio or video, of service users or members of staff. If such recordings were felt to be necessary for the investigation of suspected serious malpractice or a criminal offence this would need to be approved by the Senior Information Risk Owner or Caldicott Guardian in conjunction with NHS Counter Fraud, with police involvement where necessary, and would be subject to the Regulation of Investigatory Powers Act 2000[1]. Any such recording would be for a specific, documented purpose and limited to a specified timeframe.

Staff should not undertake covert recordings of colleagues or service users without being specifically authorised to do so by the Trust. If staff have concerns which they believe need to be investigated they should raise them with their line manager or other appropriate manager in accordance with the Speaking Up – Freedom to speak up: Raising Concerns (Whistleblowing) Policy.

Members of staff are not permitted to make covert recordings of colleagues or service users for their own purposes whilst at work. Anyone making such recordings in contravention of this policy would be personally responsible for any breach of Data Protection legislation.

[1] Regulation of Investigatory Powers Act 2000 (legislation.gov.uk)

7.2 Recording of Consultations by Service Users or Carers

Service users and/or carers are not encouraged to record consultations with professionals but there may be instances where they wish to make recordings to which they can refer back and so may record consultations unless to do so would be detrimental to staff or service user safety, or detrimental to the care and treatment of the service user.

If service users or carers make recordings, they are responsible for maintaining the confidentiality of their own information.

Where the professional is aware that a recording is being made, the service user or carer should be reminded of the private and confidential nature of the recording and that it is their responsibility to keep it safe and secure. The professional should clarify that any recording is only made for personal use and that the misuse of a recording may result in criminal or civil proceedings.

The professional may request that they are not visible in any video recording.

If the professional believes that the recording could be detrimental to the treatment of the service user or that it could pose a risk to the safety of the service user or the professional (for instance if it was posted online) then they may terminate the consultation unless the recording is stopped.

7.3 Recordings of Staff or Service Users on Wards

Service users are not permitted to make audio or video recordings of other service users, visitors or staff performing their duties on inpatient wards. They should be informed of this on admission to the ward or as soon as practical thereafter.

Similarly, visitors to wards are not permitted to make recordings on the ward.

If staff become aware of service users making any such recordings they will ask the service user to delete the recording from their device and staff will witness the deletion.

If the service user persists in making recordings, the device being used may be confiscated for the duration of their stay on the ward.

If visitors are found to be making recordings on the ward they will be asked to stop and to delete the recordings. If they refuse they will be asked to leave the ward.

Unauthorised recordings by service users will be recorded as incidents via the SHSC incident recording process.

7.4 Use of Surveillance Cameras

The Trust may use surveillance cameras to record on Trust premises where it is deemed necessary to protect the safety of service users and staff, or to deter violence or investigate serious incidents.

Surveillance cameras will only be used when less-intrusive methods would not be sufficient to achieve the stated aim(s) of the cameras.

Any proposed installation of surveillance cameras must be subject to a Data Protection Impact Assessment and must be approved by the appropriate Trust information governance group before it may commence.

Where surveillance cameras are used, information will be provided to staff, service users and visitors informing them about the use of cameras, their purpose, the identity of the data controller and data subjects' rights including the process for making subject access requests for recordings.

Information recorded by surveillance cameras does not form part of the care record. Any information from the recording which is relevant to the care record of service users must be transcribed separately into the care record.

See the separate CCTV/Surveillance Camera policy for more detail.

7.5 Recording of Telephone Conversations

The Trust may record telephone conversations in case they are needed for the completion of records or the investigation of incidents.

Where telephone conversations are routinely recorded the caller will be informed of this fact by a standard announcement before being connected.

Recordings of telephone calls do not form part of the care record – any information which is relevant to the care record must be transcribed into the care record promptly.

Where there is a need to record telephone conversations covertly for the investigation of a suspected offence this must be approved by the Senior Information Risk Officer or Caldicott Guardian in conjunction with NHS Counter Fraud, with police involvement where necessary, and would be subject to the Regulation of Investigatory Powers Act 2000.

7.6 Recording of Skype/Teams telemedicine sessions/consultations

Remote consultations by Skype or similar services, whether video or audio only, will be treated in the same way as telephone conversations – recordings of them will not be retained as part of the care record so any relevant information from them must be documented in the care record. Recordings of remote consultations may be stored for a limited time for the completion of records or the investigation of incidents.

If sessions are recorded the service user will be informed of this fact.

Care must be taken when setting up calls to ensure that any recordings are stored securely and that access to them is restricted on a need-to-know basis.

7.7 Recordings of staff and/or service users for training or publicity

Where audio or video recordings or photos of service users or staff are required to be used for training or publicity this must be with the explicit, informed consent of the subject – contact the Communications department for details of the necessary consent forms.

7.8 Recording of sessions by trainees for assessment by supervisors

Recordings may be made as part of professional training subject to the explicit consent of the service user and subject to the service user being provided with information as to the uses of the recordings, their storage, how long they will be kept for and who will be able to access them. The service user will also be given the right to withdraw their

consent at any time and provided with information on how to do this. Any such recordings must be transferred to the assessor or supervisor by means of a secure process approved by the SHSC IT Department.

7.9 Recording of Meetings

Recording may be of use for lengthy meetings and hearings to aid the accuracy of minute or note taking over a long period. It may also be useful for evidential purposes during official Trust hearings (such as appeals or employment hearings). Such recordings do not replace the formal record of any meeting, but may assist with the accuracy of the formal record or if there is dispute over what was said. It is also advisable to have a minute or note taker in attendance in the event of a technology failure.

Those attending meetings or hearings must be informed in advance of the intention to record the proceedings. This advance notification is helpful in avoiding any issues on the day. Any objections to the recording must be considered by the Chair who will ultimately decide whether the recording is appropriate in light of any objection. At the meeting, the Chair must also notify all attendees that recording will take place prior to the commencement of the recording. The recording must stop at the formal close of the meeting or hearing. Attendees who were not present at the start of the meeting must also be notified that recording is taking place when they join. Covert recordings must not be taken and to do so will be considered a disciplinary offence.

7.10 Retention of Recordings

Recordings containing personal-identifiable information will be subject to the same requirements as other person-identifiable records.

They must be stored securely, including any held on mobile devices. Retention periods are set out in the NHS Records Management Code of Practice although recordings will not generally form part of the care record.

7.11 Access to Recordings

Recordings containing personal-identifiable information are covered by Subject Access rights provided by Data Protection legislation.

Subject Access requests are processed and monitored by the Information Governance Team. Forms are provided to expedite the processing of requests but data subjects can make verbal requests to the organisation if the prefer. There is no fee for requests and they should be answered within one month of receipt unless the request is complex, so staff should notify the Information Governance Team promptly if they receive a request.

8 Development, Consultation and Approval

This policy was developed at the request of the Data & Information Governance Group (DIGG).

It was submitted to the Clinical Operations Meeting for comment in April 2019.

It was further revised in light of comments from Data & Information Governance Group members in December 2019.

It was reviewed and updated in January 2023.

9 Audit, Monitoring and Review

This section should describe how the implementation and impact of the policy will be monitored and audited. It should include timescales and frequency of audits.

If the policy is required to meet a particular standard, it must say how and when compliance with the standard will be audited.

Monitoring Compliance Template						
Minimum Requirement	Process for Monitoring	Responsible Individual/ group/committee	Frequency of Monitoring	Review of Results process (e.g. who does this?)	Responsible Individual/group/ committee for action plan development	Responsible Individual/group/ committee for action plan monitoring and implementation
Compliance with this policy	Review as part of the Data Security & Protection Toolkit assessment	Data & Information Governance Group	Annual	Data & Information Governance Group	Data & Information Governance Group	Data & Information Governance Group

Policy documents should be reviewed every three years or earlier where legislation dictates or practices change.
Review date: 31 January 2026.

10 Implementation Plan

All policies should include an outline implementation plan (this will summarise sections 7, 8 and 9 above). It should include consideration of:

- *Dissemination, storage and archiving*
- *Training and development requirements and who will provide the training*
- *Any new job roles and responsibilities and how these will be implemented*
- *Resources needed*
- *Timescales*
- *Lead role and responsibilities for implementation*
- *Audit or monitoring of implementation planned*

The implementation plan should be presented as an action plan and include clear actions, lead roles, resources needed and timescales. The Director of Corporate Governance team can provide advice on formats for action plans however; an example layout for the plan is shown below:

Action / Task	**Responsible Person**	**Deadline**	**Progress update**
Upload new policy onto intranet and remove old version	Communications Dept.	03/2023	
Make team aware of revised policy	Team managers	Ongoing	

11 Dissemination, Storage and Archiving (Control)

This section should describe how the new policy will be disseminated. It says where the policy will be made available and to whom. This will normally be that the policy is available on the Trust's intranet and available to all staff.

It makes it plain that any previous versions must be deleted and describes the archiving and storage arrangements for the current and previous versions of the policy.

It says who is responsible for archiving and version control, and what they should do.

Version	Date on website (intranet and internet)	Date of "all SHSC staff" email	Any other promotion/ dissemination (include dates)
1.2	12/02/2020	Feb 2020	
1.3			

12 Training and Other Resource Implications

Departmental managers are responsible for ensuring that their staff are aware of and comply with this policy.

13 Links to Other Policies, Standards (Associated Documents)

Data & Information Security Policy
Remote Working and Mobile Devices Policy Data & Information Acceptable Use Policy
Records Management Policy
Mobile Phones, Communication Devices and Internet Access for Service Users
Confidentiality Code of Conduct
CCTV/Surveillance Camera Policy
Data Protection Act 2018/ UK General Data Protection Regulation Regulation of Investigatory Powers Act 2000
NHSx Records Management Code of Practice 2021

14 Contact Details

Title	***Name***	***Phone***	***Email***
Information Governance Manager	Katie Hunter	2716723	katie.hunter@shsc.nhs.uk
Data Protection Officer	John Wolstenholme	3050749	john.wolstenholme@shsc.nhs.uk

Appendix A

Equality Impact Assessment Process and Record for Written Policies

Stage 1 – **Relevance** - Is the policy potentially relevant to equality i.e. will this policy potentially impact on staff, patients or the public? This should be considered as part of the Case of Need for new policies.

NO – No further action is required – please sign and date the following statement. **I confirm that this policy does not impact on staff, patients or the public.**	***I confirm that this policy does not impact on staff, patients or the public.*** Name/Date: J Wolstenholme, 23/01/2023	**YES,** Go to **Stage 2**

Stage 2 Policy Screening and Drafting Policy - Public authorities are legally required to have 'due regard' to eliminating discrimination, advancing equal opportunity and fostering good relations in relation to people who share certain 'protected characteristics' and those that do not. The following table should be used to consider this and inform changes to the policy (indicate yes/no/ don't know and note reasons). Please see the SHSC Guidance and Flow Chart.

Stage 3 – **Policy Revision** - Make amendments to the policy or identify any remedial action required and record any action planned in the policy implementation plan section

SCREENING RECORD	Does any aspect of this policy or potentially discriminate against this group?	Can equality of opportunity for this group be improved through this policy or changes to this policy?	Can this policy be amended so that it works to enhance relations between people in this group and people not in this group?
Age			
Disability			
Gender Reassignment			
Pregnancy and Maternity			

Race			
Religion or Belief			
Sex			
Sexual Orientation			
Marriage or Civil Partnership			

Please delete as appropriate: - Policy Amended / Action Identified (see Implementation Plan) / no changes made.

Impact Assessment Completed by:
Name /Date

Appendix B

Review/New Policy Checklist

This checklist to be used as part of the development or review of a policy and presented to the Policy Governance Group (PGG) with the revised policy.

		Tick to confirm
	Engagement	
1.	Is the Executive Lead sighted on the development/review of the policy?	✓
2.	Is the local Policy Champion member sighted on the development/review of the policy?	✓
	Development and Consultation	
3.	If the policy is a new policy, has the development of the policy been approved through the Case for Need approval process?	N/A
4.	Is there evidence of consultation with all relevant services, partners and other relevant bodies?	✓
5.	Has the policy been discussed and agreed by the local governance groups?	✓
6.	Have any relevant recommendations from Internal Audit or other relevant bodies been taken into account in preparing the policy?	✓
	Template Compliance	
7.	Has the version control/storage section been updated?	✓
8.	Is the policy title clear and unambiguous?	✓
9.	Is the policy in Arial font 12?	✓
10.	Have page numbers been inserted?	✓
11.	Has the policy been quality checked for spelling errors, links, accuracy?	✓
	Policy Content	
12.	Is the purpose of the policy clear?	✓
13.	Does the policy comply with requirements of the CQC or other relevant bodies? (where appropriate)	✓
14.	Does the policy reflect changes as a result of lessons identified from incidents, complaints, near misses, etc.?	✓
15.	Where appropriate, does the policy contain a list of definitions of terms used?	✓
16.	Does the policy include any references to other associated policies and key documents?	✓
17.	Has the EIA Form been completed (Appendix 1)?	✓
	Dissemination, Implementation, Review and Audit Compliance	
18.	Does the dissemination plan identify how the policy will be implemented?	✓
19.	Does the dissemination plan include the necessary training/support to ensure compliance?	✓
20.	Is there a plan to i. review ii. audit compliance with the document?	✓
21.	Is the review date identified, and is it appropriate and justifiable?	✓