

Audio, Visual & Photographic Recordings Procedure

At a glance ...

- Audio and video recordings can be intrusive to the privacy of individuals. Their use must be necessary, proportionate and adequate.
- Service areas considering changing business processes to include the routine use of audio or video recordings of service users should undertake a [summary Data Protection Impact Assessment](#)
- Participants must be told in advance if a meeting is to be recorded. At the start of the meeting the Chair must advise that recording will take place, the purpose/s of it, who it will be shared with and signpost to privacy information.
- The status of the recording should be clear, particularly whether it will be retained as the sole record of the meeting or is used to inform written notes / minutes and will be destroyed once these have been approved.
- In the unlikely event that the Council needs to rely on the consent of individuals to undertake recordings, there must be evidence of having obtained it (through a consent form or via the recording).
- All recording devices and recordings must be kept secure at all times and comply with the [Acceptable Use Standard](#).
- Portable recording devices must be [destroyed securely](#) at the end of their lifespan. Recordings must be destroyed securely at the end of their retention period.
- Where a portable audio recording device is required, only audio recording devices supplied by ICT Services may be used and these must have a sufficient level of security, including encryption.
- If a portable device or audio recording is lost, stolen or damaged to the point of recordings being irretrievable, or if recordings have been subject to unauthorised access, this must be [reported as a data breach](#).
- A member of staff must take responsibility for a recording and must:
 - transfer data to a suitable NCC network location within one working day of the recording taking place;
 - use the recommended naming convention for the file and check its quality and completeness
 - where applicable, delete the recording from recording device following successful transfer to the network location.
- Requests for audio/video recordings by people asking for their own data (i.e. a Subject Access Request) or as part of Freedom of Information request will be referred to the Complaints and Information Team or HR where it relates to employees or former employees.

Introduction

1. The Council uses audio, visual and photographic recordings of staff, service users and members of the public for a variety of purposes, as part of its daily work. Photographic film, digital images and video and audio recordings such as tapes, digital dictation and recording devices are all used. Audio and/or video of virtual meetings held via MS Teams may also be recorded.
2. Recordings that identify living individuals are subject to the General Data Protection Regulation and Data Protection Act 2018.
3. This procedure details Council responsibilities towards service users, staff and members of the public about the use of visual and audio recordings and to ensure that all recording that takes place is done:
 - For a clear purpose.
 - With consent (where this is occasionally required)
 - To ensure safe, responsible and secure use, storage and transportation of recordings.

Purpose of this document

4. The purpose of this document is to detail procedures on the appropriate use of audio, visual and photographic recordings by Council staff to ensure compliance with the Data Protection Act 2018, other relevant legislation and associated Council policies, guidance and standards.
5. This document complements other documents which reference audio, visual and photographic recordings including:
 - [Surveillance Camera \(CCTV\) Procedure](#) which sets out Council standards and approach for the use of surveillance camera systems (including CCTV, drones, body worn cameras etc)
 - [Taking Photographs with Mobile Devices Guidance](#)
6. It forms part of the Council's [Information Governance Framework](#) and sits under the [Information Compliance Policy](#).

Scope and definitions

7. The principles and commitments set out in this procedure apply to all members, employees, trainees / apprentices and volunteers of the County Council and to contractors, suppliers and partners delivering County Council services on our behalf.
8. Members of the Council should note that they are also data controllers in their own right and are responsible for ensuring any personal information they hold/use in their role as Members is treated in accordance with the relevant legislation.

9. This procedure does not apply to recordings under the Police and Criminal Evidence Act (PACE) 1984 which have separate and detailed codes of practice.
10. This procedure does not apply to information held by schools who are individually responsible for ensuring that they comply with Data Protection and Freedom of Information legislation. If a request concerns data protection in a school or a wish to access school records, the requester should contact the Head Teacher of the relevant school.
11. An audio recording device is defined as related hardware and software for recording, processing and storing the data which is captured.
12. Information or data in this procedure is used as a collective term primarily to describe personal data collected using audio recording devices.

Principles & Commitments

Informing meeting participants that audio/visual recording will take place

13. If pre-arranged meetings are to be recorded, written invitations to meetings should inform the participants (see example [Invitation to a Review Child Protection Conference letter](#) at Appendix A)
14. Meeting Chairs should inform all meeting participants at the beginning of the meeting that recording will take place, the purpose/s of the recording and who it will be shared with inside and outside the Council.
15. It is important that the status of the recording is understood. If the recording functions as “notes” to inform the written record and be destroyed thereafter then it can be treated as any other notes. All parties to the panel should be informed that the proceedings will be recorded, the recording is used to inform the written record of the meeting and then destroyed. Information on where privacy notice information can be referred to should also be provided (this is <https://www.nottinghamshire.gov.uk/global-content/privacy>).
16. Data minimisation is key principle of Data Protection legislation. This means that a written and digital copy of the same meeting should only be held as the formal record where there is a specific justification.
17. Individual business areas must have clear procedures around the destruction of the recording, and this should typically be done no later than one week after the formal written note has been agreed (to enable time to review the recording and make any required amendments to the written note).
18. Service areas considering changing business processes to include the routine use of audio and/or video recordings of service users should undertake a [summary Data Protection Impact Assessment](#) and seek advice from the Information Governance Team.

Individual’s consent to the use of audio, visual and photographic recordings

19. We will only rely on consent as a condition for processing personal data if there is no relevant legal power or other condition.
20. The Council has extensive powers and so it is likely consent will not be required in most cases but there may be exceptions, such as where recordings are made for communications, publicity or marketing. Where it is required, [consent](#) must be sought.
21. If you are unsure if you require the consent of an individual you should contact the Information Governance team for advice data.protection@nottsc.gov.uk.
22. Consent should generally be documented using the [media consent form](#).
23. Consent may be recorded at the beginning of an audio or visual recording, as part of the recording
24. For consent to be valid the individual must be told the following:
 - the name of the organisation;
 - the name of any organisations with whom the data will be shared
 - why you want the data;
 - what you will do with it;
 - where privacy information can be obtained; and
 - that individuals can withdraw consent at any time (note: that where consent is relied on to process recording and is later withdrawn, the Council may also be required to delete the recording upon request).

Use of devices for audio, visual and photographic recordings

25. All personal and confidential information must be kept safe and secure at all times, including at the office, public areas, home or in transit, in compliance with the [Information Compliance Policy](#).
26. All devices storing or processing NCC data must be approved for use by ICT in accordance with the [Acceptable Use Standard](#).
27. Staff must not use any devices to store or process NCC data that have not been supplied to individual business areas, and configured, by ICT Services. ICT Service will implement a process to ensure that there are suitable controls for the supply of, and support to, audio recording devices.
28. Passwords for removable media encryption must be in accordance with the [Password Standard](#).
29. The member of staff responsible for the recording must ensure they password-protect access to the recording devices.
30. All removable media including, but not limited to, USB drives and memory cards, must be encrypted in compliance with the [Encryption Standard](#).

31. The member of staff responsible for the recording must ensure they encrypt recordings, when necessary.
32. The business area responsible must have local procedures in place regarding what members of staff should do if a device issued to them is lost, stolen or damaged. The Meeting Support Service has an extensive suite of local procedures which could be obtained and adapted for this purpose.
33. If a device is lost, stolen or damaged to the point of recordings being irretrievable, or if there is reason to believe that data on the device has been subject to unauthorised access, this must be [reported to the Information Governance Team as a data breach](#) in line with the Data Security Incident and Breach Management Procedure.
34. Further advice regarding taking photographs of service users is available in [Taking Photographs with Mobile Devices](#).
35. Additional guidance and procedures for the use of overt CCTV usage is available through the [Surveillance Camera / CCTV Procedure](#). All use of overt surveillance and CCTV must comply with this procedure.
36. The use of covert CCTV usage is subject to the [Regulation of Investigatory Powers Act 2000](#) (RIPA). Authorisation for covert surveillance is required prior to recording taking place. The procedure for authorisation can be found in the council's [Covert surveillance and RIPA](#) page.

Removal of recordings from devices

37. The member of staff responsible for the recording must ensure they transfer data to an NCC network drive or SharePoint site within one working day of the recording taking place.
38. The member of staff responsible for the recording must ensure they check the quality and completeness of the transferred recording.
39. The member of staff responsible for the recording must ensure they delete recordings from recording devices following successful transfer to an NCC network drive or SharePoint site.
40. **Recordings must not be stored on desktop or local PC drives. This includes personal Onedrive accounts.**

Retention of recordings

41. Recording devices automatically assign names to new files created, which are meaningless when stored and do not easily allow for searches in relation to Subject Access Requests. The member of staff responsible for the recording must ensure audio and visual recording files are renamed using the following naming convention:
 - Date of recording (yyyymmdd)
 - Name of data subject (recordings involving data subjects) **OR**

- Staff or Mosaic number assigned to data subject
- Name of third-party organisation **OR**
- Name of topic/subject matter

42. For example, a recording involving a service user or member of staff would be named 20190505 Jane Doe. In the case of more than one recording involving the person during the same date files can be renamed 20190505 Jane Doe1, 20190505 Jane Doe2, etc.

43. Using identification numbers, a recording involving a service user or member of staff would be named 20190505 Mosaic 12345. In the case of more than one recording involving the person during the same date files can be renamed 20190505 Mosaic 12345a, 20190505 Mosaic 12345b, etc.

44. Files involving third party organisations can be named on the same principle; 20190505 Acme1, etc.

45. The member of staff responsible for the recording must ensure the recording is retained in accordance with the Council's [Records Retention and Disposal Schedule](#).

46. The member of staff responsible for the recording must ensure the recording is labelled in accordance with the Council's [Information Security Classification Standard](#).

Access to and sharing of recordings

47. Access to recordings will be based on a need-to-know basis and in accordance with relevant legislation and Council policies and procedures.

48. Requests from NCC staff to access recordings made by another business area will be handled by the business area responsible for the recording. There must be a legitimate reason to give access which takes account of Data Protection law. Advice should be sought from the Information Governance Team where the position is unclear. Where access is granted a record of this should be kept.

49. Requests from individuals or their representatives for access to, or copies of, their personal data, will be referred to the Complaints & Information team.

50. Subject Access Requests and more general Information Rights Requests will be centrally coordinated as set out in the [Subject Access Requests](#) and [Data Subject Rights](#) Procedures.

51. Requests by third parties, other than Subject Access requests, for access to or copies of personal or confidential recordings will be responded to confidentially, securely, legally and consistently and in line with our service standards and procedures. This will include:

- a) Use of secure email and encryption for sending electronic information and tracking for paper documents.

- b) Ensuring that Information Sharing Agreements and Data Processing Agreements are in place, for routine sharing where deemed necessary and that the terms of those agreements are observed.
- c) That personal data is only shared with external bodies where there is an Information Sharing Agreement or other legal basis for sharing.
- d) Maintaining a documented log of the request and the data shared.
- e) That personal data is not shared with an individual or organisation based in any country outside of the European Economic Area (EEA) unless there is express permission to do so following a Data Protection Impact Assessment.

52. Individuals are permitted to request audio and video recordings under the Freedom of Information (FOI) Act 2000. The Council's Complaints and Information Team coordinates FOI requests for the Council and will also coordinate any audio data required as part of a FOI. Exemptions under the FOI Act will continue to apply; this can include refusing the disclosure of a recording if it includes personal data.

Disposal of recording devices

53. Devices no longer suitable for use must be returned to ICT for [secure disposal](#) in line with the [Data Destruction Standard](#).

Training

54. All those using recording devices should be issued with documented guidance/manuals concerning their use.

55. Guidance/manuals should include instructions on password protecting the devices and/or encrypting recordings.

56. Staff should seek advice from their line manager if further training or guidance is required, who will arrange further training or support.

Responsibilities

57. Duties assigned to specific roles referenced in this procedure must be carried out as described below. The Council's [Information Governance Framework](#) provides further detail of the nature of specific information governance related roles (e.g. that of SIRO, Caldicott Guardian, Data Protection Officer etc.) see also the intranet page on [IG roles and responsibilities](#).

Staff member/group	Responsibility
Information Governance Board	Approving this procedure. Approval of subsequent reviews will ordinarily be undertaken by the Procedures and Standards Sub-Group of the Information Governance Board. The Data Protection Officer (DPO) may approve minor amendments.
Data Protection Officer	Establishing arrangements to monitor and report on compliance with this procedure and provide support, advice and training.
ICT Services	To approve the use of all devices storing or processing NCC data, in accordance with the Acceptable Use

Staff member/group	Responsibility
	<p>Standard.</p> <p>To ensure instructions on password protecting the devices and/or encrypting recordings are available on the NCC intranet.</p> <p>To ensure documented guidance / manuals on the use of the recording devices are available for all users.</p>
Complaints and Information Team manager	Maintaining a record of all Subject Access Requests (SARs) and Freedom of Information Act (FOIA) requests, coordinating responses and managing liaison with requestor (except Human Resources SARs).
Communications & Marketing team	To manage the Asset Bank Photographic Library To maintain the Media consent form
HR Service	Maintaining record of all SARs related to personnel records and managing liaison with requestor (Human Resources records).
All managers	To implement this procedure and ensure their teams are aware of and comply with this procedure. To ensure their teams are made aware of local storage and retention procedures for recordings.
All staff	All staff using the devices for recording, or having access to recordings, to comply with this and related procedures.

Compliance with this Procedure

58. Wilful or negligent disregard for information governance policies and procedures will be investigated and may be treated as a disciplinary matter under the relevant employment procedure(s) which could lead to dismissal or the termination of work agreement or service contracts.

Review

59. This procedure will be periodically monitored and reviewed by the Data Protection Officer (or their nominee) who will revise it in line with learning arising from the implementation of the procedure, legislation and codes of good practice.

60. Beyond that, the procedure will be monitored and reviewed every three years.

Related legislation

61. Related legislation includes:

- [General Data Protection Regulation](#)
- [Data Protection Act 2018](#)
- [Human Rights Act 1998](#)
- [Regulation of Investigatory Powers Act 2000](#)
- [Digital Economy Act 2017](#)
- [Police and Criminal Evidence Act 1984](#)

Related Council policies/strategies/frameworks/programmes, partnership agreements etc.

62. Related Council policies/strategies/frameworks/programmes, partnership agreements include:

- [Information Governance Framework](#)
- [Information Compliance Policy](#)
- [Information Rights Policy](#)
- [Information Security Policy](#)
- [Acceptable Use Standard](#)
- [Encryption Standard](#)
- [Information Security Classification Standard](#)
- [Password Standard](#)
- [Records retention and disposals schedule](#)
- [Using photos, video and audio](#)
- [Video or teleconference recordings](#)
- [Media consent form](#)
- [Taking Photographs with Mobile Devices](#)
- [Open surveillance and CCTV](#)
- [Surveillance Camera Process and Guidance](#)
- [Covert surveillance and RIPA](#)
- [Regulation of Investigatory Powers Act and Surveillance Guidance – covert surveillance, ‘directed’ surveillance and Covert Human Intelligence Sources \(CHIS\)](#)
- [Data Destruction Standard](#)
- [Subject Access Requests Procedure](#)
- [Data Subject Right Procedure](#)

Advice, Support & Further Information

63. Further advice about this procedure can be obtained from:

<p>Information Governance Team Email: data.protection@nottscc.gov.uk Telephone: 0115 8043800</p>	<p>Complaints & Information Team Email: accessto.records@nottscc.gov.uk Telephone: 0115 9772788</p>
--	--

64. Further reading and supporting information:

Title (as hypertext link) and publication date	Author
Data Protection and Audio Recordings	Information Commissioner’s Office (ICO)


Document Control

Owner	Data Protection Officer
Original Author	William Smith, Information Manager
Last Reviewer	Tim Boden

Approver	Data Protection Officer (DPO)
Date of Approval	24/06/2022
Date of next review	23/06/2025
Version	1.3
Classification	Public

Version	Date	Changes and Approver
1.0	05/09/2019	Approved by Information Governance Group. Drafted in consultation with Meetings Support Service (MSS) and HR.
1.1	26/10/2019	Minor changes made and approved by DPO under delegation from IGB. ICT, MSS role clearer, DPIAs and PACE referenced.
1.2	15/11/2019	Minor change – edited link to go to latest edition of Taking Photographs with Mobile Devices guidance. Approved by DPO.
1.3	24/06/2022	Updated to reflect the increased use of MS Teams and associated recording of meetings. Approved by DPO.

Appendices

An Invitation to a Review Child Protection Conference letter	 Parent RCPC Invite 2019.docx
--	--