London School of Economics & Political Science

Information Management and Technology (IMT)

Guidelines

Audio and Video Recording

Jia Fu
Information Security Officer

Summary	Guidelines for data protection around audio and video recording
Version	Release 1.0
Date	27 Janaury 2017
Library reference	IMT-GD-103

Table of contents

1 Introduction

1.1 Background

The School's Information Security Classification Standard and the Research Ethics Policy require proper arrangements to be made around the security of research data.

It has been noted that digital audio and video recording is increasingly adopted by LSE staff and students as a method of enhancing their research activities, such as conducting interviews during research fieldwork. Most recorded interviews will contain sensitive personal data, the disclosure of which not only is against ethical research duties, but also can cause financial and reputational loss to the LSE. The fines can be up to £500,000 under the UK Data Protection Act (DPA), or, up to 4% of LSE's worldwide turnover under the EU's General Data Protection Regulation (GDPR)*.

It is in light of this that the present Guidance has been developed, with a view to provide practical advice around each stage of the audio and video recording process, thereby helping LSE staff and students to fulfil their ethical, policy, and legal duties.

[NOTE] This Guidance may be further tightened in relation to any development of the School's arrangements towards compliance with the upcoming GDPR.

1.2 How to use this Guidance

This Guidance is in the format of an overview Flowchart that shapes out the audio and video recording flow, followed with the same Flowchart but along with guidance notes at key steps. There are reference numbers at some steps, for which you can find further explanations or references in Section 3 of this Guidance.

1.3 Scope

In light of the objective of this Guidance as explained in above Section 1.1, this Guidance focuses on the digital audio and video recording of interviews with living individuals as part of research work, where LSE staff or student carries out such recording, or otherwise shares the audio/video and / or the transcription files.

If deemed as necessary, this Guidance can be referred to during other similar data collection procedures such as focus group discussions, workshops, panel discussions, etc.

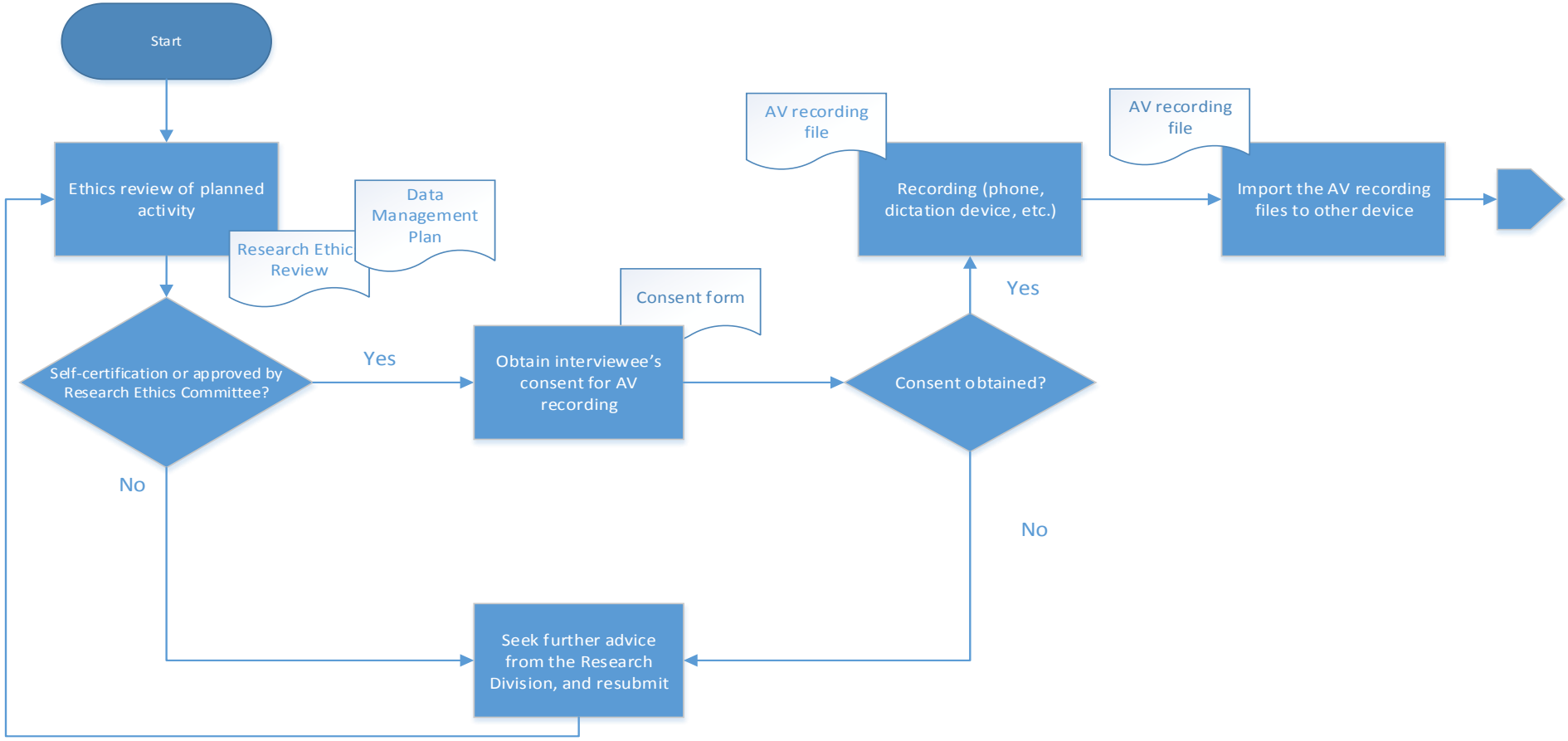
1.4 Out of Scope

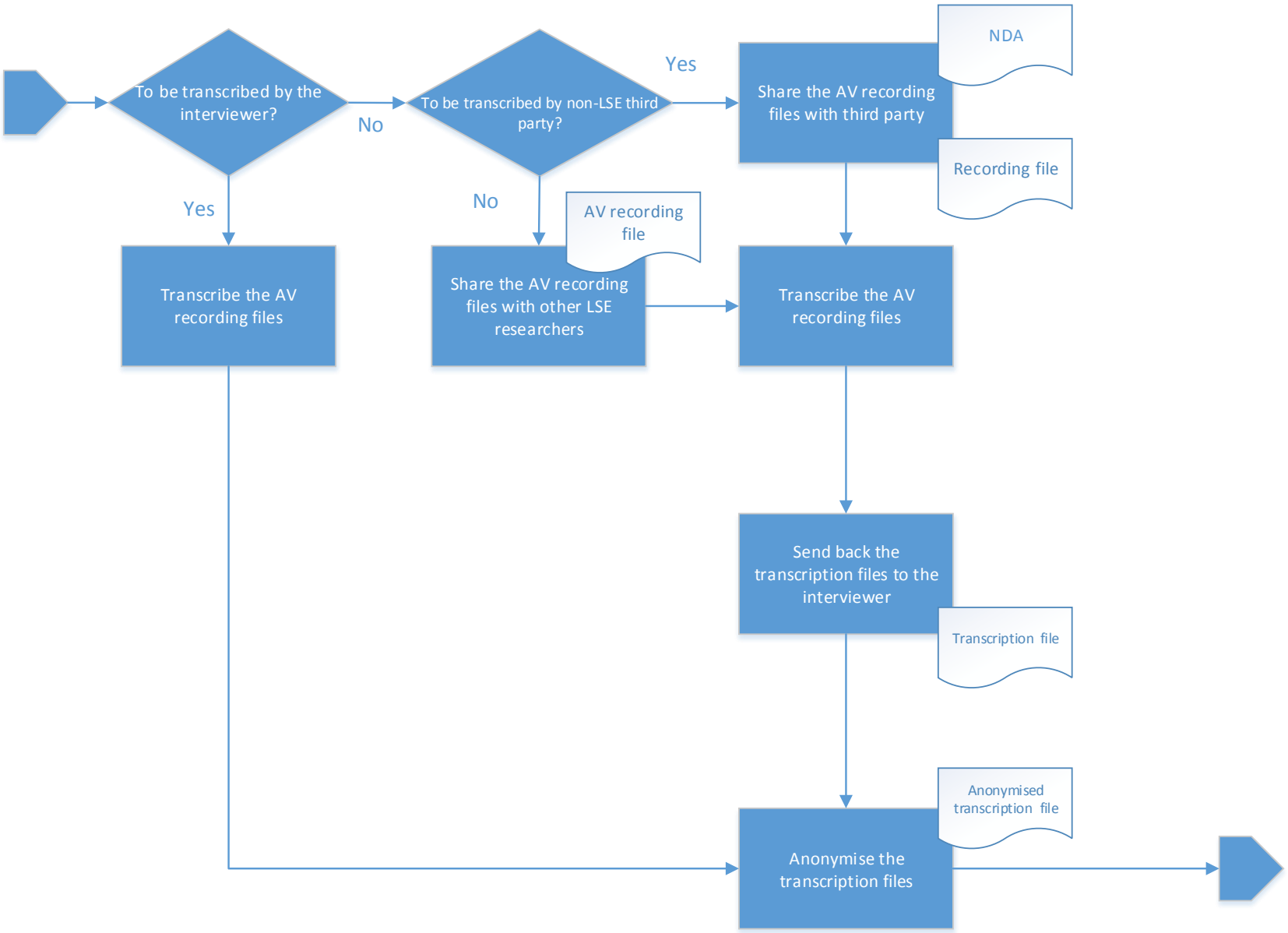
This Guidance does NOT apply to recordings made available by LSE through its public video and audio channels.

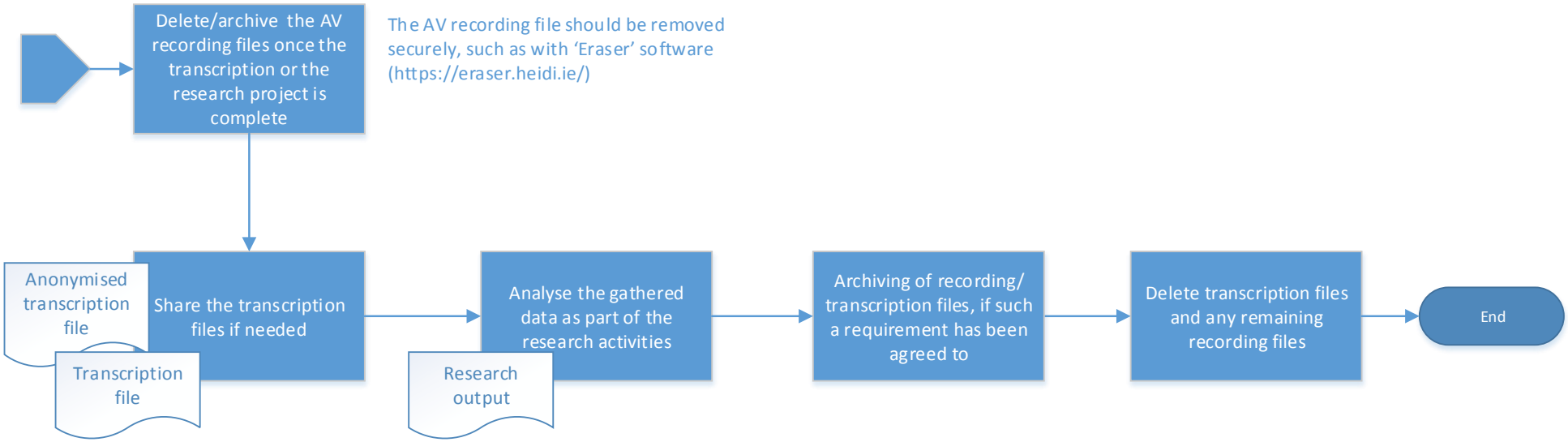
For avoidance of doubt, the protection measures addressed in this Guidance can be superseded by the tighter contractual requirements agreed with third parties such as the research funder.

2. Guidance

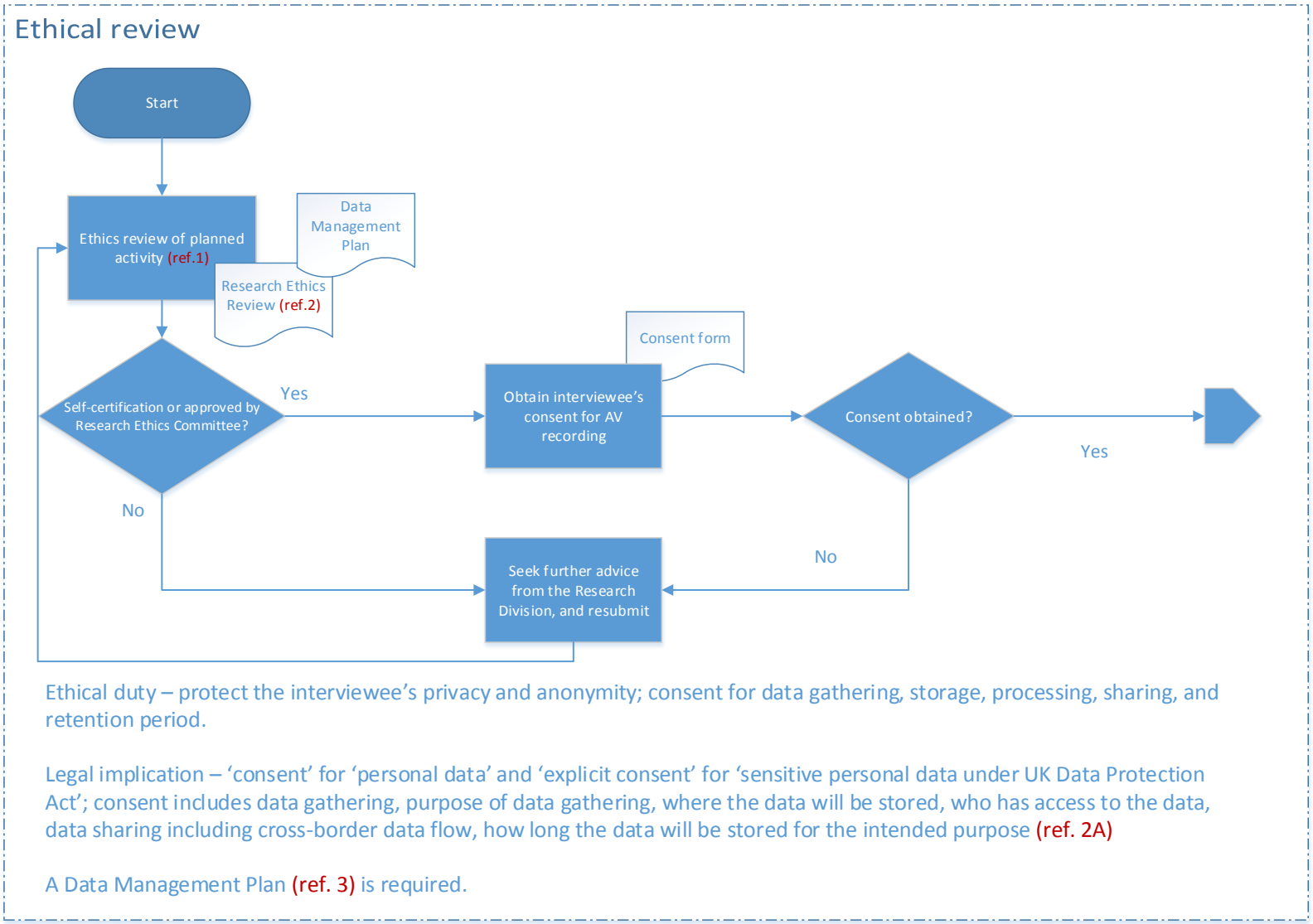
2.1 Overview




To be transcribed by the interviewer?
No
To be transcribed by non-LSE third party?
Yes
Share the AV recording files with third party
NDA
Recording file
Yes
Transcribe the AV recording files
No
AV recording file
Share the AV recording files with other LSE researchers
Transcribe the AV recording files
Send back the transcription files to the interviewer
Transcription file
Anonymised transcription file
Anonymise the transcription files


Delete/archive the AV recording files once the transcription or the research project is complete
The AV recording file should be removed securely, such as with 'Eraser' software (https://eraser.heidi.ie/)
Anonymised transcription file
Transcription file
Share the transcription files if needed
Research output
Analyse the gathered data as part of the research activities
Archiving of recording/ transcription files, if such a requirement has been agreed to
Delete transcription files and any remaining recording files
End

2.2. Guidance notes

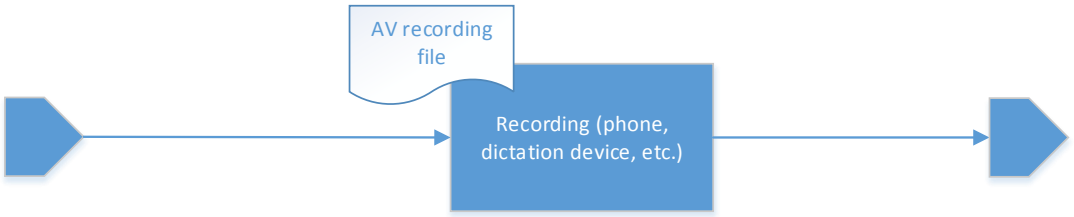


Ethical duty – protect the interviewee's privacy and anonymity; consent for data gathering, storage, processing, sharing, and retention period.

Legal implication – 'consent' for 'personal data' and 'explicit consent' for 'sensitive personal data under UK Data Protection Act'; consent includes data gathering, purpose of data gathering, where the data will be stored, who has access to the data, data sharing including cross-border data flow, how long the data will be stored for the intended purpose (ref. 2A)

A Data Management Plan (ref. 3) is required.

Recording device



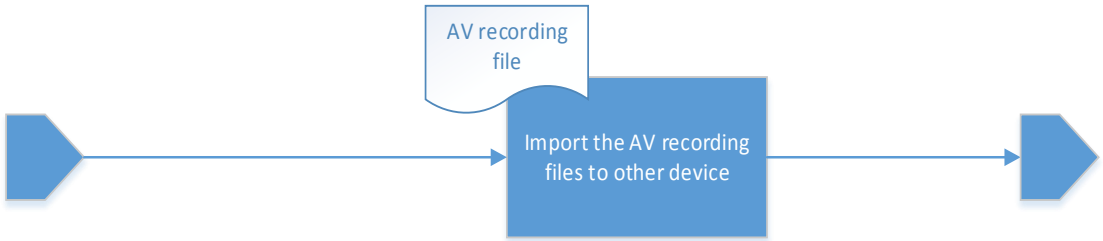
If the recording contains 'sensitive personal data' under the DPA (ref.7), or is considered as confidential where leakage of data represents medium to high risk, then dictation device with real-time encryption capabilities should be used, with no internet connection to the device during the recording process (note that as long as a device is connected to Internet it opens up potential communication channels to the device, thereby the risk of compromise through these channels).

Otherwise, a phone can be used with full drive encryption applied (both iOS and Android have such features). (ref. 4) Optional extra layer of security can be added by locking down the particular folder that contains the sensitive data – this depends on the available apps for iOS and Android system.

Where possible, transfer the files from the phone to other devices (e.g. PC) as soon as recording is complete (note that Android phone is particularly vulnerable comparing to iOS devices, due to the way Android system, as an 'open' platform (vs. 'closed' Apple device), pushes out systems and software updates and it's relatively loose controls over the Operating System and apps downloads. That said, no device is definitively secure; for instance the iOS device is more targeted than ever along with its increased popularity).

Consider the physical security of the recording device while unattended – dictation device should be locked up; phone is fully encrypted; 'remote wipe' is enabled where possible.

Recording files

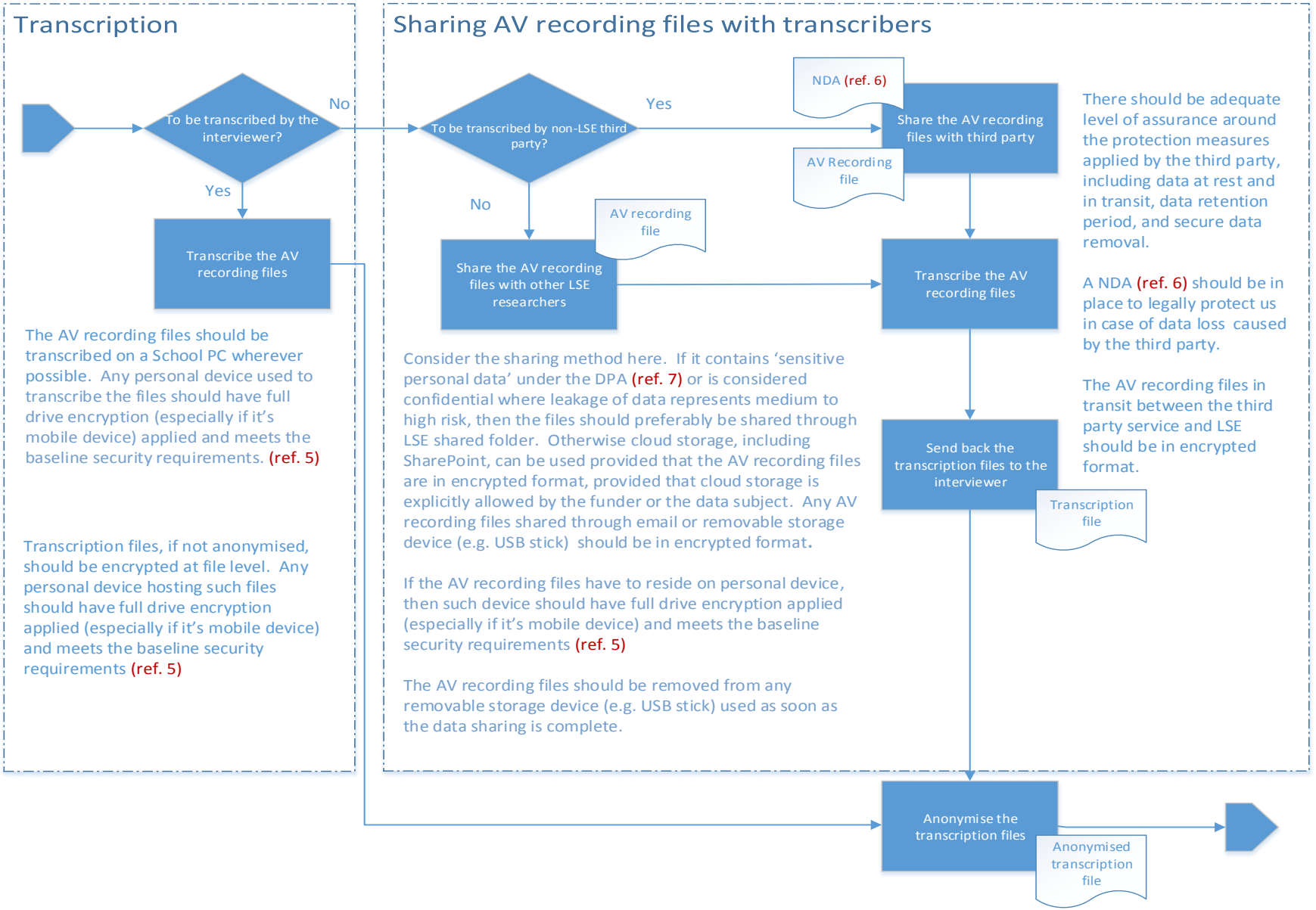


Consider both device level and files level security:

Device level – ideally the audio recording file should be residing at a School PC / the School network; if not possible, full device encryption (especially mobile device) should be applied and baseline security requirements met (ref.5). Also consider the physical security of the device while unattended.

File level – apply encryption at file/folder level.

As soon as the AV recording files are moved they should be permanently deleted from the recording device.



Transcription

The AV recording files should be transcribed on a School PC wherever possible. Any personal device used to transcribe the files should have full drive encryption (especially if it's mobile device) applied and meets the baseline security requirements. (ref. 5)

Transcription files, if not anonymised, should be encrypted at file level. Any personal device hosting such files should have full drive encryption applied (especially if it's mobile device) and meets the baseline security requirements (ref. 5)

Sharing AV recording files with transcribers

Consider the sharing method here. If it contains 'sensitive personal data' under the DPA (ref. 7) or is considered confidential where leakage of data represents medium to high risk, then the files should preferably be shared through LSE shared folder. Otherwise cloud storage, including SharePoint, can be used provided that the AV recording files are in encrypted format, provided that cloud storage is explicitly allowed by the funder or the data subject. Any AV recording files shared through email or removable storage device (e.g. USB stick) should be in encrypted format.

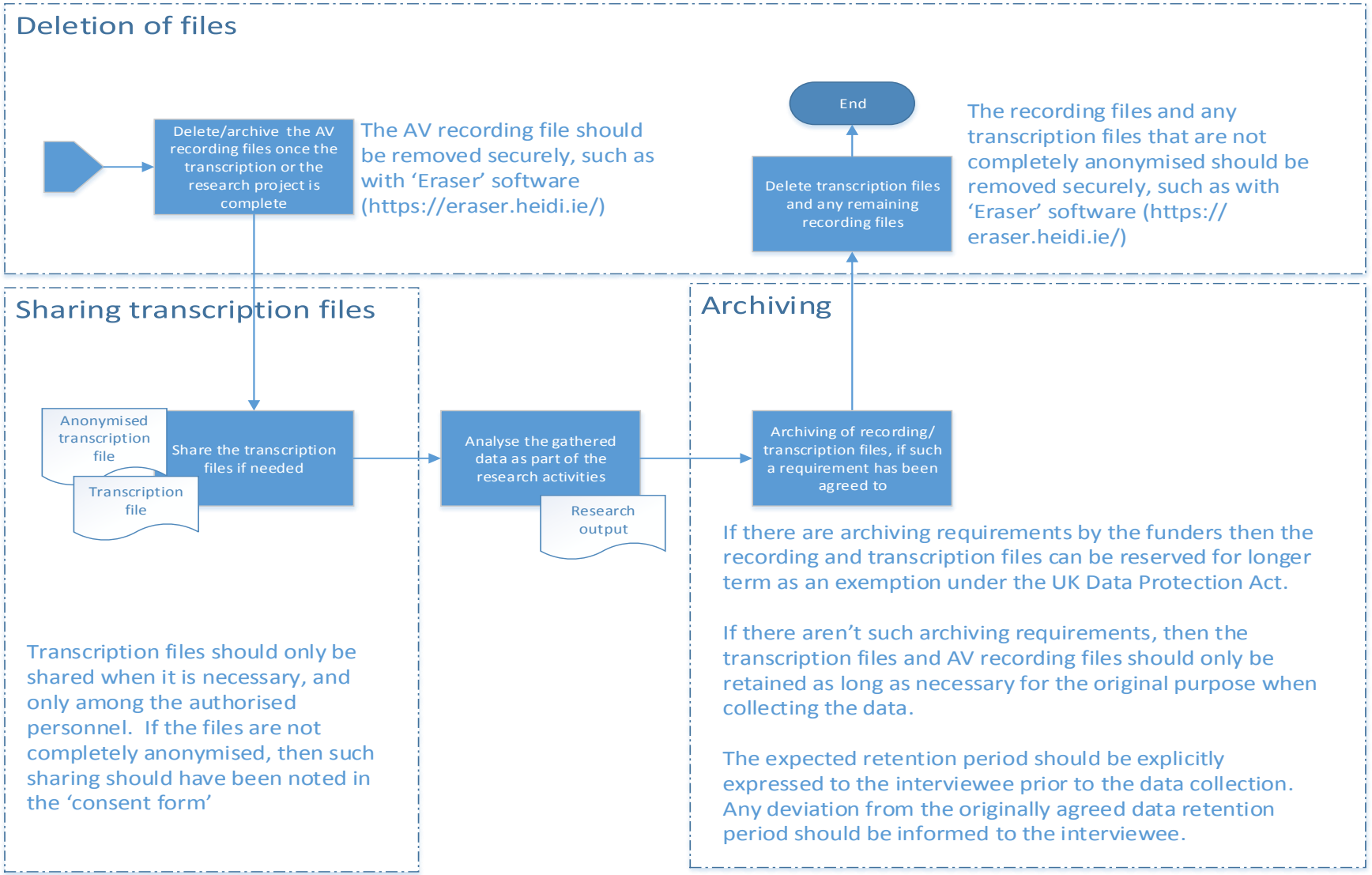
If the AV recording files have to reside on personal device, then such device should have full drive encryption applied (especially if it's mobile device) and meets the baseline security requirements (ref. 5)

The AV recording files should be removed from any removable storage device (e.g. USB stick) used as soon as the data sharing is complete.

There should be adequate level of assurance around the protection measures applied by the third party, including data at rest and in transit, data retention period, and secure data removal.

A NDA (ref. 6) should be in place to legally protect us in case of data loss caused by the third party.

The AV recording files in transit between the third party service and LSE should be in encrypted format.


Deletion of files
Delete/archive the AV recording files once the transcription or the research project is complete
The AV recording file should be removed securely, such as with 'Eraser' software (https://eraser.heidi.ie/)
End
Delete transcription files and any remaining recording files
The recording files and any transcription files that are not completely anonymised should be removed securely, such as with 'Eraser' software (https://eraser.heidi.ie/)
Sharing transcription files
Anonymised transcription file
Transcription file
Share the transcription files if needed
Analyse the gathered data as part of the research activities
Research output
Archiving of recording/ transcription files, if such a requirement has been agreed to
Archiving
Transcription files should only be shared when it is necessary, and only among the authorised personnel. If the files are not completely anonymised, then such sharing should have been noted in the 'consent form'
If there are archiving requirements by the funders then the recording and transcription files can be reserved for longer term as an exemption under the UK Data Protection Act.
If there aren't such archiving requirements, then the transcription files and AV recording files should only be retained as long as necessary for the original purpose when collecting the data.
The expected retention period should be explicitly expressed to the interviewee prior to the data collection. Any deviation from the originally agreed data retention period should be informed to the interviewee.

3. Reference notes

Ref. 1
Research Ethics Policy – please read through the Research Ethics Policy and Procedures at http://www.lse.ac.uk/intranet/LSEServices/policies/pdfs/school/resEthPolPro.pdf

Ref. 2
Research Ethics Review – please refer to Annex B of the document linked in Ref. 1

Ref. 2A
DPA Section 33 exception does allow that data may be retained indefinitely provided it is processed only for academic 'research purposes'

Ref. 3
Data Management Plan (DMP) – please read through the guidance around the DMP at http://www.lse.ac.uk/library/usingTheLibrary/academicSupport/RDM/planning/dataManagementPlanning.aspx

Ref. 4
Please refer to LSE's encryption guideline at
http://www.lse.ac.uk/intranet/LSEServices/IMT/about/policies/documents/Guidelines-Encryption-Guidelines-v1-1.pdf
http://www.lse.ac.uk/intranet/LSEServices/IMT/about/policies/documents/encryptionGuidelinesStudents.pdf

Ref. 5
Device-level baseline security requirements:

- Explicit password to log on
- Full device encryption is applied if it's a mobile device / laptop (Bitlocker or VeraCrypt for Windows, FileVault for Mac)
- Password to log on or the hard drive encryption key is complex (8 digits minimum length and a combination of upper and lower case characters, numbers, Non-alphanumeric characters)
- Actively operate anti-virus software
- Actively operate a software firewall (enable the built-in firewall option in the operating system)
- Keep the operating systems up to date by installing security patches as soon as they are released
- Keep other software up to date by implementing security patches as soon as they are released
- Apply a screen saver (e.g. after 5 minutes' inactivity)
- Enable the 'remotely wipe data' option if available
- Exercise reasonable care to prevent the shoulder surfing attack (can consider applying a privacy screen filter)

Ref. 6
Non-Disclosure Agreement (NDA) – please find the template at
http://www.lse.ac.uk/intranet/LSEServices/IMT/about/policies/documents/SampleNDA-Final.pdf

Ref. 7
For definition of 'sensitive personal data' under the Data Protection Act, please refer to the School's Data Protection Policy at
http://www.lse.ac.uk/intranet/LSEServices/policies/pdfs/school/datProPol.pdf

4. Other issues

4.1 Further Policies, Codes of Practice, Procedures and Guidelines

These guidelines sit beneath LSE's overarching *Information Security Policy*. Other supporting policies have been developed to strengthen and reinforce these guidelines. These, along with associated codes of practice, procedures and guidelines are published together and are available for viewing on LSE's website. All staff, students and any third parties authorised to access LSE's network or computing facilities are required to familiarise themselves with these supporting documents and to adhere to them in the working environment.

The below list of current policies is in no way authoritative and new policies will be published on the LSE website as they become available.

Associated polices:

Conditions of Use of IT Facilities at LSE
Policy on the use of mobile telephony equipment
Policy on the use of school-funded iPhones
Password Policy
Data Protection Policy
Research Ethics Policy
Code of Research Conduct

Standards and Guidelines:

Information Classification Standardz
Remote Access and Mobile Working Guidelines
Guidelines on the use of Cloud storage
How do I encrypt my stuff?