MANCHESTER 1824
The University of Manchester

**Standard Operating Procedure**

| | | | |
|---|---|---|---|
| **Title:** | Taking recordings of participants for research projects | | |
| **Version:** | 1.0 | **Effective Date** | October 2018 |
| **Summary** | Procedure for secure handling of recordings and transcriptions | | |

**When using this document please ensure that the version you are using is the most up to date by checking on the University's online document system http://documents.manchester.ac.uk/list.aspx for any new versions.**

## 1 Background and purpose

As part of their work and studies at the University, some staff and students may need to record interviews or other activities involving participants. Still and moving images and sound recordings featuring identifiable individuals contain the personal data of the participants and therefore must be processed in accordance with data protection laws. The University is the Data Controller for all such images and recordings regardless of where the recordings take place. The University determines the purpose of recording and is legally responsible and accountable for its use.

The purpose of this Standard Operating Procedure ("Procedure") is to provide clarity regarding the recording, transfer, storage, analysis, retention and disposition of audio and video data in order to protect the privacy of participants and to ensure that valuable research data is also protected in terms of its confidentiality, integrity and availability.

## 2 Definitions and scope

- **Personal data**: Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.
- **Special Category Data**: Personal data which the General Data Protection Regulation says is more sensitive, and so needs more protection including information about an individual's race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (where used for ID purposes), health, sex life or sexual orientation, information relating to criminal convictions and offences.
- **Identifiable**: Able to be named or recognised
- **Pseudonymisation:** The processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information.
- **Anonymisation:** The irreversible process of turning data into a form which does not identify individuals.
- **Disposition:** The final stage of records management in which a record is either destroyed or permanently retained.
- **Data Controller:** A person or organisation who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
- **Data Processor:** Any person or third party organisation (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller.

- **Processing:** Includes recording, transfer, storage, analysis, retention and disposition of audio, video and image data.
- **Recordings:** May include video (moving picture), audio (sound), or photograph (image) using a variety of methods such as camera, camcorder, smartphone, voice note, Skype, Adobe Connect, etc.
- **Transcription:** Involves converting the recording into a written format.
- **Participants:** Individuals who are the subject of the recording; they are data subjects in data protection law.
- **Data Custodian:** A Data Custodian is an employee of the University who has administrative and/or operational responsibility for research information. The Data Custodian is the person who manages the information on a regular basis. Data Custodians are responsible for the safe custody, transport, storage of the data and implementation of business rules.
- **Principal Investigator**: The Principal Investigator (PI) is a University member of staff that has overall responsibility for the preparation, conduct, administrative and financial management and reporting of a research project. In the case of collaborative research led by an external organisation, the PI is the member of University staff leading the activities for which the University is responsible.
- **Student Supervisors:** University and external staff involved in supervising University-registered students. Within a supervisory team, the main academic supervisor is a University member of staff and has full responsibility for the overall management and direction of the student's research degree in addition to administrative issues relating to the student's registration, attendance, and progress.
- **Ethical Approval**: Favourable opinion from a properly constituted ethics committee. University research requiring ethical approval will need approval from either a Health Research Authority Research Ethics Committees ('NHS REC') or University of Manchester Research Ethics Committee ('UREC').
- **Research:** It is generally understood that research is the use of a systematic and sound methodology to answer questions or generate new hypotheses in order to make an original contribution to knowledge. Research projects may be conducted by undergraduate and taught postgraduate students to fulfil the requirements of their programme of study. These projects are not necessarily intended to make an original contribution to knowledge. However, for the purposes of this SOP, such projects are classed as research.
- **Intellectual Property:** The collective term to describe various different rights protecting intellectual creations, such as patents, trademarks, designs and copyright. Ownership rights in relation to IP are contained in the University's Intellectual Property Policy.
- **Confidentiality:** Concerned with preserving authorised restrictions on information access and disclosure, including the protection of personal data and proprietary information.
- **Integrity:** Concerned with guarding against improper information modification or destruction and ensuring the authenticity of any changes.
- **Availability**: Concerned with ensuring timely and reliable access to and use of information.

This Procedure applies to:

- All individuals conducting research in the name of the University ("researchers"). This includes members of staff, students and collaborators as well as individuals conducting research at or for the University and/or its subsidiaries, who are duly authorised to have access to University data including the transcription of recordings. This includes staff who have temporary, honorary, visiting, casual or voluntary status with the University; agency workers; students employed by the University; and suppliers. This list is not intended to be exhaustive.
- Recordings created for research purposes.

## 3 Procedure and responsibilities

### 3.1 Consequence of non-compliance with this Procedure

Compliance with this Procedure is mandatory and non-compliance must be reported to the Head of Information Governance who will determine the action to be taken. Breaches may be referred to the Head of Research Governance, Ethics and Integrity for consideration under the University's procedures for investigating potential research misconduct. The Information Governance Office or Research Governance team will report all breaches to the Head of the appropriate School. Staff and students must note that any breach of this Procedure may be treated as misconduct under the University's relevant disciplinary procedures and could lead to disciplinary action. Serious breaches of this Procedure may constitute gross misconduct and lead to summary dismissal.

### 3.2 Participants' rights

It is essential that participants are informed of their rights in relation to the recording. A Participant Information Sheet (PIS) must provide sufficient information about the use of their recording. An example of the kind of topics to be included in the PIS can be found in the template on the University's document centre.

### 3.3 Responsibilities

- **The Associate Vice President for Compliance, Risk and Research Integrity** is chair of the University's Research Compliance Committee which receives reports from the URECs and oversees compliance with regulations and legislation that govern the use of humans in research.
- **The University Research Ethics Committees** undertake an ethical review of any relevant research project in the University with a view to:
    - maintaining ethical standards of practice in research;
    - protecting participants of research and researchers from harm;
    - preserving the participants' rights and welfare; and
    - providing reassurance to the public and to outside bodies that this is being done.
- **Research Governance Sponsor Representative** – acts on behalf of the University (Research Governance Sponsor) for all University-led research conducted under the UK Policy Framework for Health and Social Care Research ('UK Policy Framework'). Ensures that researchers are aware of their responsibilities under the UK Policy Framework and, through a research governance review undertaken for all studies, the proposed research is carried out in accordance with University policies and procedures.
- **Heads of School, Directors or equivalent** are responsible for ensuring that all staff within their area act in accordance with this Procedure.
- **Research IT** will provide the technical infrastructure and support to enable the appropriate management of the participant recordings.
- **Information Asset Owners**- IAOs are accountable for the information being processed.
- **Supervisors and/or Principal Investigators (PI)** are the Information Asset Owner for the project (see Information Security Classification, Ownership and Secure Information Handling SOP). The responsibility for information provided by participants always rests with the supervisor and/or PI as the University is legally responsible for the data.

- **Students -** Where students are undertaking the research, arrangements for the management of research data and records must be discussed and agreed between the student and the supervisor, and the student is expected to abide by the agreements reached.
- **All authorised users** of information are responsible for its safe custody. Anyone who has access to information whether as a user of a software application or as a recipient of information via digital, paper or verbal means, is required to keep the information secure to the level required by the Information Asset Owner.

**3.4 Approval of proposed recording and transcription activities:**

Ethical approval must be obtained before commencing any recording.

Prior to approval the Supervisor/Principal Investigator must ensure that, for each element of information to be gathered, the following have been considered:

- The recording must be limited to the information necessary to address the aims of the research project;
- The structure of the recording must be planned in advance so far as is appropriate to the research project;
- The need for audio recording as opposed to taking field notes and/or the need to use a video recording as opposed to an audio recording has been justified; and
- Any new requests to purchase recording equipment must be for encrypted devices as advised by Research IT, and the cost of such equipment must be included in funding applications.

Details of the proposed recording must be included in the full mandatory Data Management Plan completed for the research project. Additionally, the end-to-end data handling of these recordings must be documented eg by completing a data flow diagram or narrative. Approved storage for research data can be found here. If it is not possible to meet the storage requirements, a review of the Data Management Plan must be requested via DMP Online and any questions directed to Research IT via the tool.

The PI/Supervisor must sign to confirm that they understand and will comply with this Procedure either through the Ethical Review Manager tool or the faculty research governance review process.

**3.5 Recording participants - instructions**

- Only record what has been approved by the ethics committee as necessary for the study;
- Ensure the location of any recording is appropriate eg consider the privacy and comfort of the participant and/or any risk involved;
- Where possible the name of the interviewee must not be recorded unless verbal consent is required and this must be recorded separately from the interview;
- An encrypted University-provided device must be used for recording eg an Apple iOS device such as an iPod touch, iPhone or iPad which has been enrolled onto the University Exchange email service to activate device encryption.
- In exceptional circumstances, where high quality audio, twin microphones and more than one recording device (eg for backup) are required, it may be permissible to use a device that is not encrypted but explicit approval must be given by the ethics committee and data must be downloaded to an encrypted device and deleted from the unencrypted device as soon as possible. The advice of Research IT must be obtained before buying a recording device;

- The device used to make the recording must never be left unattended and must be locked away securely when not in use; and
- If a recording device is shared, any recordings must be deleted prior to handing over to another user.

### 3.6 Transfer of recordings to University storage

- Recordings must be transferred from the recording device to University storage (as detailed in the Data Management Plan) as soon as possible to ensure that a master copy is backed up and the file is encrypted.
- Recordings should be checked once transferred and before deleting from the recording device.
- Examples of methods for transferring recordings securely to University storage can be found in Appendix A.

### 3.7 Storage of recordings

- Transcripts must be securely stored ie on servers provided through IT Services ("University servers").
- Appropriate storage must be used as per the information security classification of the data captured, as well as any third party data providers' requirements.
- Approved storage for research data can be found here. Data must be encrypted to AES 256 standard when not in use. Further University of Manchester guidance on file encryption can be found here.
- Highly restricted information must always be encrypted, including data on University systems and with third-party/cloud service providers.[1]
- Transcripts not held on University servers must be stored on an encrypted device for temporary storage only. They must be transferred to University servers and deleted from temporary storage as soon as possible. Information regarding hardware encrypted USB sticks can be found here: http://www.itservices.manchester.ac.uk/secure-it/encryption/usb/

### 3.8 Processing the recordings (eg coding, analysis, transcription)

- The identity of the participant must be anonymised in the transcript as soon as is practicable;
- The transcription of recordings must be done in a secure environment where the data subject cannot be seen or heard by another person outside the approved team. Anonymised recordings do not require the same level of security. Further information regarding the minimum security controls can be found in the "Information security classification, ownership and secure information handling SOP";
- Transcription by a third-party is only permitted where either a University-approved transcription service is used or the ethics committee has agreed that transcription can be conducted by students as part of their studies.
- Transcription by students requires a signed confidentiality agreement. A template confidentiality agreement can be found in Appendix B.

### 3.9 Data transfer, collaboration or sharing

[1] Information Security Classification, Ownership and Secure Information Handling Standard Operating Procedure.

If recordings that contain personal data are moved to another organisation, a data transfer agreement must be in place between the organisations, particularly where it is not possible to anonymise the data eg observational studies. This also applies when staff leave the University and request to take the data with them, and may apply if staff move within the University. See Appendix A for guidance on transfer.

### 3.10 Retention and disposition

Information must be kept in accordance with the University's Retention Schedule and Research Data Management Plan. Destruction of records must be performed in a secure manner, ensuring that records to be destroyed are transported securely and destroyed completely in a manner that renders the information completely and irreversibly destroyed. Further information regarding disposal of confidential material can be found here.

### 3.11 Incident reporting

If recordings or transcripts that have not been anonymised are lost, stolen, corrupted or disclosed to, or accessed by, unauthorised persons, it must be reported to the Head of Information Governance as soon as possible in order that appropriate measures can be taken to contain any damage and minimise the harm which might arise.

Contact the Information Governance Office:
Email: infosec@listserv.manchester.ac.uk
Telephone: 0161 275 7789

## 4 Monitoring compliance with the Procedure

### 4.1 Enforcement

Heads of Schools, Directors or equivalent are responsible for obtaining assurance that all staff within their area act in accordance with this procedure.

### 4.2 Audit

Awareness of this Procedure will be audited periodically.

### 4.3 Reporting

The Head of Information Governance will report on the Procedure to the Information Governance Committee.

The Head of Research Governance, Ethics and Integrity will report breaches of this Procedure to the Research Compliance Committee.

## 5 Review of Procedure

This Procedure will be reviewed at least every two years or when significant changes are required.

## 6 Contact list for queries related to this procedure

| Role | Name | Telephone | Email |
|---|---|---|---|
| Head of Information Governance | Tony Brown | 0161 306 2106 | Tony.brown@manchester.ac.uk |
| Head of Research Governance, Ethics and Integrity | April Lockyer | 0161 275 8093 | April.lockyer@manchester.ac.uk |

| **Document control box** | |
|---|---|
| Procedure title: | Standard Operating Procedure – Taking recordings of participants for research projects |
| Version: | 1.0 |
| Date approved: | 4 October 2018 |
| Approved by: | Information Governance Committee |
| Supersedes: | New |
| Next review date: | October 2020 |
| Related Statutes, Ordinances, General Regulations | • Ordinance XIV Intellectual Property Rights (IPR), Data Protection and the Use of Information Systems<br>• University General Regulation XV Use of Information Systems |
| Related policies and procedures: | • Information security policy: http://documents.manchester.ac.uk/display.aspx?DocID=6525<br>• Information Security Classification, Ownership and Secure Information Handling SOP: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=29971<br>• Information Security –Responsibilities SOP: http://documents.manchester.ac.uk/display.aspx?DocID=8039<br>• Template Participant Information Sheet: http://documents.manchester.ac.uk/display.aspx?DocID=37215 |
| Policy owner: | Head of Information Governance/ Head of Research Governance Ethics and Integrity |

| Version | Date | Reason for change |
|---|---|---|
| 1.0 | October 2018 | Creation |

**APPENDIX A**

**Guidance for transferring data from recording devices to University of Manchester storage**

- Recordings must be transferred from the recording device to University storage (as detailed in the Data Management Plan) as soon as possible to ensure that a master copy is backed up and the file is encrypted.
- Recordings should be checked once transferred and before deleting from the recording device.

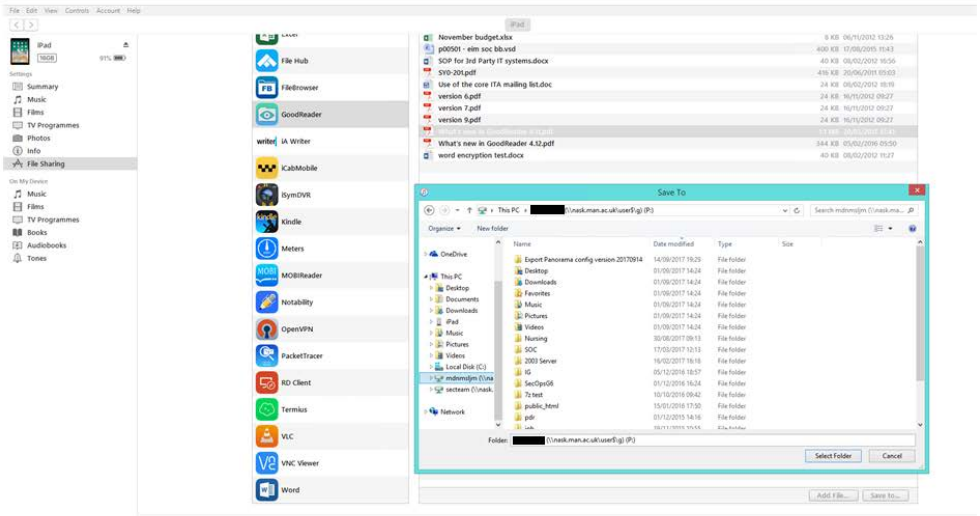
**1 Guidance on how device tools can be used to transfer data is provided below.**

1.1 Apple Devices

When using University-provided Apple devices such as iPads the following process using iTunes can be used.

The transfer process using iTunes requires the iTunes application installing on your University of Manchester PC to make a connection from your iPad to your PC via the USB data/charging cable. Once connected, you can then transfer data from a compatible iPad app as per this Apple knowledge base article: https://support.apple.com/kb/PH20348?locale=en_US

This enables a direct transfer from the iPad to the PC, or network storage mapped to the PC such as the P drive or a shared drive. The process must not involve transferring the data to iCloud or any other third-party hosted cloud service. Please see the screenshot below for an example of using iTunes to transfer a PDF from the GoodReader app on an iPad directly to the P Drive using the 'save to' button at the bottom right of the screen.



1.2 Video Recorders

There are no mass-produced camcorders with built-in encryption capabilities. Therefore, when using a camcorder to record sensitive data alternative security measures will need to be implemented. The camcorder must be stored in a locked location when not in use. The data must be transferred from any insecure portable media at the end of every recording session or day, whichever is more appropriate, to University storage (see section 3.6 and 3.7). If this is not possible it must be stored on an encrypted medium until it is possible to move to University storage. If stored on an unencrypted drive, the video files must be encrypted following University guidance on file encryption, which can be found here. Once the transfer is complete, the videos on the media used in the camcorder, eg SD card, must be wiped with a secure deletion utility.

## 2 Transfer of data to University of Manchester or External Collaborators

The following tools can be used to transfer data to the University of Manchester or External Collaborators:

- University of Manchester Dropbox Service – Data must be encrypted before storing on the service. Please read the terms and conditions of use of this service at: http://www.itservices.manchester.ac.uk/ourservices/catalogue/commscollab/sec/
- Zendto – Data must be encrypted before sending via Zendto. More information on the Zendto service can be found at: https://zendto.manchester.ac.uk/

**APPENDIX B**

## Confidentiality Agreement for Transcription

This agreement is intended for use when University of Manchester staff or students are transcribing audio/video recordings for University-led research studies. **It is not to be used with external transcription service providers.**

**To be completed by the research team:**

| | |
|---|---|
| **Study title:** | |
| **Study Principal Investigator (PI)** | |
| **Study Data Custodian** (if different than PI) | |
| **Data Management Plan reference** | |

**To be completed by the transcriber:**

**[Highlighted sections should be updated by the research team before use. Highlighting, this guidance note and [] should not be present in the final version]**

I understand that I will be [hearing/viewing] [audio/video/etc.] recordings of [interviews/focus groups/etc.] that have been conducted for the above study. I understand the information contained in the recording(s) has been provided by research participants who have taken part in the research with the assurance that their information will remain strictly confidential. I understand my responsibility to maintain confidentiality and confirm I will adhere to the terms outlined below.

| | **Please Initial** |
|---|---|
| I agree to keep the content of the audio/video recording(s) confidential and not discuss the content of the recording(s) or transcript(s) with anyone other than [insert PI/data custodian or name of researcher that will liaise with transcriber on behalf of PI/data custodian]. | |
| I agree to keep the recording(s) secure when in my possession and to follow all specific instructions provided by [insert PI/data custodian or researcher name] in relation to storing, transcribing and transferring the recording(s). | |
| I agree to return all research information when I have completed the agreed transcription tasks, as per [insert data custodian/researcher name] instructions. | |
| I agree to erase or destroy all research information in any form or format that is not returnable, as per [insert data custodian/researcher name] instructions. | |

**Transcriber:**

| *Print Name* | *Signature* | *Date* |
|---|---|---|

**Principal Investigator/Data Custodian:**

| *Print Name* | *Signature* | *Date* |
|---|---|---|

One copy to be held by the PI/Data custodian (original); one copy for the transcriber