WH:SHF Wave 3 Guidance: Audio and Visual Data Management

Created by IFF Research

DESNZ's independent evaluation partners

The Purpose of this Guidance

As part of your self-conducted evaluation activities for Wave 3, any evidence you may collect, including resident interviews, site photography and video case studies can all help to demonstrate the impact of the Warm Homes retrofit programme. However, capturing a resident's voice or image does carry significant ethical and legal responsibilities.

The purpose of this guidance is to help you understand the best practice guidelines in ensuring:

Data Legality: Navigate the specific requirements of the UK GDPR and Data Protection Act 2018 regarding multimedia files.

Protecting Your Project: Prevent data breaches or consent withdrawals that could invalidate your evaluation findings or damage your organisation's reputation.

Maintaining Trust: Ensure residents feel safe and respected if they are sharing their homes and feedback.

This guidance will provide a practical framework for every stage of any multimedia evaluation activity you may choose to complete:

1. Ethics and regulations
2. Consent
3. Fieldwork compliance
4. Anonymisation & Redaction
5. Secure storage & disposal
6. Media checklist to ensure compliance

Why Ethics Matter

Regulatory compliance

Celebrating 60 years of IFF Research

As you are leading your own evaluation activities, you are responsible for handling participant data legally and ethically. In the UK, this is governed by the GDPR and Data Protection Act (2018).

General Data Protection Regulation (GDPR)

Data Protection Act (DPA)

Protecting Participant Privacy: Ensuring data is kept secure and used only for the evaluation

Individual Rights: Informing participants that they have the right to access, correct, or delete their data

Accountability: Ensuring you document how you process data and show you have a 'Legal Basis' for doing so.

The UK GDPR: Sets out the high-level principles for how personal data must be handled.

Enforces GDPR principles as well as UK specific rules

Data protection: The UK's data protection legislation - GOV.UK

Data Protection Act 2018

Why regulation is important ?

Regulations like the GDPR protect both researchers and the participant. Following them does more than keep everyone involved out of legal trouble, it ensures that the Wave 3 Evaluation remains credible and ethically sound.

Grant Recipient leads are responsible for ensuring all evaluation activities are following the required regulations

Key regulation points

Legislation: These are statutory rules set by policymakers that all evaluators must follow, E.g. UK GDPR & Data Protection Act 2018.

Self regulation: These are professional standards developed by Industry leaders (like the Market Research Society) to promote best practices, not just meeting the bare legal minimum.

Guidelines: These offer practical advice that help you apply codes of conduct to real-world scenarios, such as conducting research with vulnerable groups or recording interviews. Guidance on research practices can be found at the Market Research Society.

Celebrating 60 years of IFF Research

Your evaluation approach should be aligned with Industry standards.

Click on the logos to find out more

MRS™ Evidence Matters™

SRA SOCIAL RESEARCH ASSOCIATION

ESOMAR

Accountability

- You have a **responsibility** to ensure your evaluation activities are ethical and protect the safety and rights of all participants
- Good ethical practices protects the grant funding and the professional reputation of the SHF Wave 3 Evaluation

Why?

Why Ethical Practices Matters:

- ✓ Ensures high quality, reliable data
- ✓ Safeguards the reputation of both the project and Evaluation
- ✓ Upholds the rights and dignity of every participant
- ✓ Builds and maintains trust of those involved in the research

When conducting fieldwork you may be entering residents' private spaces. Their wellbeing should always be your priority. Guidance on qualitative research can be found here

Collect with purpose

During fieldwork it's important you **collect with purpose.** This means only gathering the data you actually need for the project.

Remember, participants have agreed to a specific scope; going off-script with unrelated questions risks a data breach.

Protect with passion

Data compliance isn't just a box-ticking exercise; it's a professional responsibility.

Embed data policy into your project management, by doing so keeps the Wave 3 Evaluation reputable for everyone involved

Accountability for Consortiums

In a consortium, accountability is shared but must be managed through a centralised framework, this could include for example:

- **The Lead Partner**: Acts as the primary point of contact for ethics and compliance, holding ultimate responsibility for reporting to DESNZ
- **Ethics Review Committee (ERC):** A dedicated sub-group that regularly audits fieldwork protocols and data handling
- **Compliance Audits**: Scheduled reviews of field notes, consent forms, and data storage need to take place to ensure all partners are adhering to the agreed-upon standards

What happens if something goes wrong ?

If ethical or data standards are breached, having clear steps to take will help. These could include having the following example protocols in place:

- **Participant grievance procedure**: Participants should be provided with contact details for an independent lead (outside the immediate field team) to report concerns or withdraw consent.
- **Incident response plan**: A pre-defined set of steps to contain data breaches or ethical lapses, including immediate DESNZ notification and impact mitigation measures.
- **Contractual accountability**: Legal agreements between consortium partners that clearly set out responsibilities and specify consequences for non-compliance with ethical and data protection standards.

See Slide 9 for example of incident reporting steps

Incident Handling

Incident Reporting

In the event of a data or ethical breach, the following incident protocols should be taken:

Step 1: Identification and containment

The immediate actions taken by the individual who first became aware of the incident

- **Stop immediately:** Cease the activity causing the issue.
- **Secure evidence:** Safely contain any data or material involved.
- **Initial assessment:** Quickly note key details (who, what, where, when).

Step 2: Internal notification

Ensuring the correct people within the project/ consortium are informed quickly

- Internal reporting to lead grant recipient and Internal compliance officer (if you have one)
- Partner escalation (for consortia)

Step 3: Response and assessment

- Ethics Review Committee (if part of consortium) review report and gathered information
- A risk assessment is completed to determine severity, impact and cause of data or ethical breach
- Decide on necessary actions; either corrective or preventative actions

Step 4: External notification (if necessary)

- Ensure all legal and contractual obligations to DESNZ and their partners are met, according to contractual funding agreements
- Participant update on the incident

Step 5: Corrective Actions

Focus on correcting and preventing issue from happening again

- Implement corrective actions (e.g., revise procedures, additional training, updating security protocols)
- Lead grant recipient to ensure all partners implement relevant changes
- Address issues with involved partners/personnel
- Document actions taken

Step 6: Post incident review and Learning

This final phase focuses on learnings from the event to improve future procedures

- Post incident report drafted by the ERC and share with all partners (if part of a consortium)
- Organise debrief and/or training to discuss the incident and any new procedures

Incident reporting summary

1. Identify & Contain
2. Internal Notification
3. Response & Assessment
4. External Notification
5. Corrective Action
6. Post-Incident Review

Identification & Assessment: Steps 1 to 3

Speed & Initial Action

- Halt activity
- Secure evidence
- Initial assessment
- Inform Internally
- Consortium alert
- ERC Review and Risk assessment

Resolution & Learnings: Steps 4 to 6

Oversight & Improvement

- ✓ Meet external obligations to DESNZ and their partners
- ✓ Update Participant
- ✓ Corrective actions to processes
- ✓ Ensure project team and/or Partner implementation
- ✓ Post-incident Report
- ✓ Debrief & knowledge sharing

Consent

Consent

Consent is key ! Without consent, no form of data collection should take place.

For your Wave 3 evaluation activities, this is especially important when capturing audio and video. Residents must voluntarily agree to be recorded and fully understand how their voice and image will be used, stored, and shared.

Informed consent

Fully informed on the purpose of the research

- What is the research about?
  Example*: We are recording this interview to capture your experience of…to better understand …to help improve…*
- What are the benefits of taking part?
- Who is commissioning the research?

Fully informed on what activities they'll do

- What is the methodology? (Will it involve videography or just audio-recording?)
- How much of their time do you need?
- Where will it take place?

Fully informed on how their data is used

- What will be published?
  - *Internal Use: Only seen by the evaluation team.*
  - *Closed Audience: Played at a private stakeholder meeting.*
  - *Public Facing: Uploaded to a website or social media.*
- Who will have access to data?
- When will the data be deleted?

Fully informed on their rights (e.g. withdrawing)

- Participants can withdraw at **any** time
  - *Including stopping audio recording or use of images at any time*
- Participants must be fully aware that:
  *Participation is **voluntary***
  *How their data will be **used***
- Participants can request a copy or to delete their data at any time

Explicit consent

Celebrating 60 years of IFF Research

Consent is key ! **Explicit consent** is required when collecting sensitive data, including **images, video, and audio recordings**. It allows participants to make specific choices about their involvement, for example, they may agree to be interviewed but choose **not** to be filmed or have their quotes used in public media.

Get explicit consent for…

- Visual recording: *Capturing a person's likeness (video or photography).*
- Audio recording: *If recording in public spaces, use data minimisation to remove or redact 'bystander' audio of non-participants*
- Attributed quotes: *Using a participant's exact words in reports or presentations.*
- Data sharing & Linking: *Sharing raw data with partners or linking responses to a specific individual.*
- Recontacting: *Asking permission to follow up for future evaluation phases*

Consent can be written, oral or electronic.

When you need consent for multiple areas within the project a standardised consent form like the one shown here is best. Find a similar version by visiting the knowledge hub.

Please tick each box and sign to say that you understand that:

ESSENTIAL REPORTING PERMISSION e.g. quotation usage?	☐
…taking part will involve being interviewed by an independent researcher from IFF Research	☐
…the researcher will record the interview to reduce note-taking and improve accuracy. Neither the recording nor any transcript will be transferred to CLIENT or any third party.	☐
…the research findings will not identify you by name, and none of your personal information will be shared outside the team carrying out the project at IFF Research.	☐
…your personal data will be stored securely by IFF Research for a period of ## months after the conclusion of the research, which is expected to be in END DATE. All named data, recordings and/or transcripts will then be destroyed.	☐
…you can contact IFF Research for a copy of your data, to change your data, or to withdraw from the research at any time prior to its completion.	☐
I have read the information above, have had the opportunity to ask any questions, and I agree to take part	☐

Signed:		**Date:**	
Print full name:			

IFF Research

For illustrative purposes only and should be used solely as a guide.

Ethical data handling

Understanding Data Risk Levels?

Regardless of whether data is ‘low risk’ or ‘high risk,’ all information must be handled with care.

Classifying your data helps you apply the right security measures to protect your participants.

Anonymous/ De-identified Data

Data that’s anonymous- No names or contact details are attached. There is not enough information for someone to reasonably identify an individual. **Photos, videos or voice recordings** that don’t capture sensitive characteristics are safe but examine thoroughly before making this decision.

Be aware of jigsaw identification! Combining multiple 'safe' characteristics (e.g., age, specific job title, and small department) can inadvertently identify someone

Personal Data

Personal data- Information that identifies someone directly (name/email) or indirectly (ID numbers, location data, or cross-referencing multiple data points)

‘Special Category Data

Sensitive data- This information requires extra protection as it includes data on ethnic origin, physical/mental health and religious beliefs. **Photos, videos or voice recordings** that capture any of the protected characteristics will be considered sensitive data.

Practical anonymisation guidelines

Rules to keep you and participants safe

Celebrating 60 years of IFF Research

Visual management

- Have permission before filming or photographing each area of a home
- Avoid capturing clutter, items not relevant to the retrofit
- Blur faces and distinctive tattoos
- Remove house numbers and street signs
- Crop out sensitive images (e.g. family photos)

Audio management

- Establish a clear signal (like a hand gesture) for when a resident wants the recorder paused.
- Voice de-identification: Use voice masking software to make speakers slightly less recognisable .
- When choosing tools ensure consideration of compliance with data protection laws (GDPR/Data Protection Action 2018) .

Scrubbing & Labelling

- Remove GPS location tags and other hidden data from image and audio properties before sharing.
- Scrubbing is done by redacting sensitive text, for example, how resident names can be redacted is shown below.
- Establish a naming structure (e.g. project#_ phase#) rather than using residents name in the filename.

Secure transfer and storage

Secure transfer and storage

“Dos”…

- **Device security:** Ensure phones/tablets used for capture are PIN-protected and encrypted
- **Secure capture devices:** Use encrypted recording apps or dedicated hardware rather than standard "Voice Memo" apps that may automatically sync to personal, non-secure clouds
- **Specialist hardware devices:** Unlike modern smartphones, older or basic recording devices often lack built-in encryption or PIN locks. If you're using these, make sure to use a dedicated SD card for each project, and store it securely once the session is over

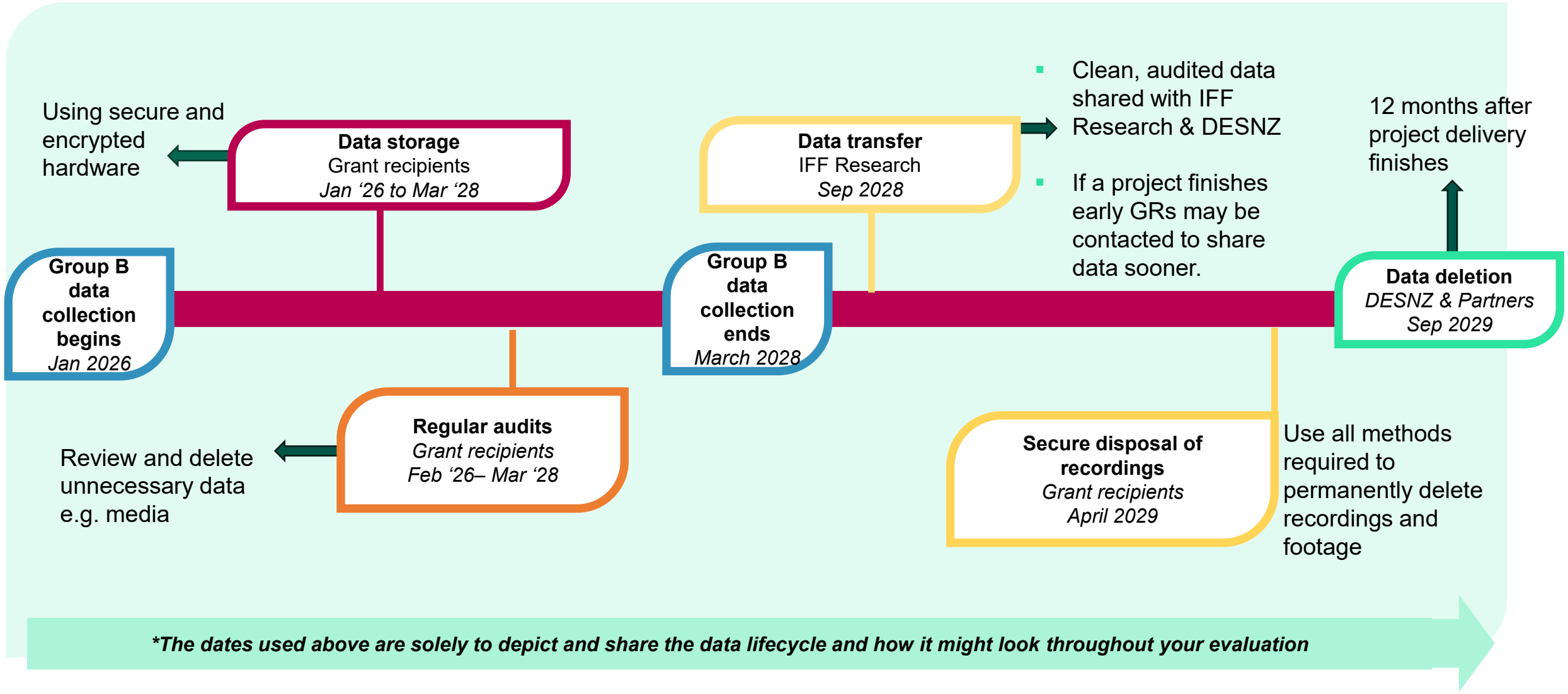
“Don’ts”…

- Use apps like WhatsApp, personal emails/devices, unencrypted USB sticks or local storage on SD cards

Apps or tools mentioned as don’ts cannot easily be regulated or monitored if they're not controlled by an organisation, this means they may not meet data protection standards and cannot guarantee compliance with GDPR.

Retention & secure disposal

How long do you need to keep data ?



The dates used above are solely to depict and share the data lifecycle and how it might look throughout your evaluation

Additional Resources

Additional Resources

Additional queries?

Contact the Evaluation support team at **shfw3_evaluationsupport@iffresearch.com**

Useful resources:

Example consent form- (link to knowledge hub to be added)

SRA GDPR guidance for social research

MRS GDPR Guidance – Section 4

Privacy notice template – Remember to tailor this to cover any audio-visual considerations for your project

Media Compliance Checklist

1. Before the recording / image capture begins

Document set up: Have you created a consent form which covers all research activity planned?

Equipment & Software: Do you have working equipment for fieldwork (audio & photography capture) and a data storage location which is GDPR compliant ?

2. Pre-Capture: The Paperwork Check

Active Consent: Has the resident signed your consent form for this research activity?

Scope Check: Does the resident understand the purpose of recording?

Opt-Out Reminder: Have you told the resident they can stop the filming/photography/ audio recording at any time without penalty?

3. During Capture: The environment check for video recording

De-Clutter PII (Personally Identifiable Information): Have you moved or framed out mail, utility bills, or prescription bottles?

Privacy Check: Are there family photos, religious symbols, or children's drawings in the background? (If yes, move the camera or the object).

Identifier Check: Is the house number or street sign visible in the shot? (It shouldn't be).

Resident Presence: If the resident is in the shot, are they dressed appropriately and comfortable with the angle?

Media Compliance Checklist continued

3. Post-Capture: The Security Check
Immediate Review: Quickly scroll through the roll, delete any accidental shots of people or sensitive data. Audio recordings cannot be deleted immediately like images, without loosing important data. At the soonest point listen back to recordings and delete sections which contain sensitive data. **Secure Upload:** Have you moved these files to the approved secure server (e.g., SharePoint)? **Local Deletion:** Once confirmed on the server, have you deleted the files from your phone/camera "Recently Deleted" folder?

REMEMBER: If the photo or recording doesn't strictly show or relate to the retrofit progress or the professional interview, it shouldn't be on your device.

Tel: 020 7250 3035

SHFW3_EvaluationSupport@iffresearch.com

www.iffresearch.com

IFF Research

@IFFResearch