Working with flood-affected people: a guide for ethical practice

Working with flood-affected people **should be read in conjunction with the webpage *How to work ethically:***
www.lancaster.ac.uk/floodarchive/how-to-guide/how-to-work-ethically

This Guide outlines ethical principles to inform how flood risk practitioners work with and collect data from flood-affected people.

These guidelines are appropriate for different types of engagement - from a one off drop-in session to a series of workshops or more sustained projects e.g. in schools or community centres. Throughout the Guide we refer to these various types of engagement by the term 'project.'

Working in all these different situations requires a sensitive and inclusive approach.

Here you will see important issues connected to three stages of engagement: before, during and after data collection.

Key ethical elements that apply to all projects are:

- Informed consent
- Avoidance of harm
- Benefits must outweigh any risks
- Right to withdraw
- Protection of personal data (confidentiality) and personal details (anonymity)

Please reference as *Working with flood-affected people: a guide for ethical practice*, Lancaster University

Stage 1 - Before Collecting Data

Before collecting any data, authorities/practitioners should consider issues of **access, safeguarding and health and safety**.

a) **Ethical approval** is currently not a requirement for flood risk practitioners/authorities but is something to consider for future practice. Academic researchers are required to gain approval from the ethics panel of their institution before undertaking any data collection. This involves explaining to the panel the data collection process and all ethical issues arising from working with people.

b) If working with a group such as a school or community group, you will need first to request **permission** from the appropriate authority (e.g. headteacher or community lead). It's important to discuss the collection methods with this authority so they are fully informed as to your plans; this helps to ensure the proposed approach is appropriate and safe for that group. You will also need to learn about the ethical guidelines already in use in that setting relating to images and recordings. You should discuss this at the outset with the lead authority.

c) You will also need to be familiar with, and follow, the school or community group **safeguarding guidelines**, which may include having an enhanced level Disclosure and Barring Service (DBS) certificate, depending on the particular circumstances.

d) You will need to create **publicity information** for participants appropriate to their age group and role (children, young people, their parents/carers, teachers etc.). If working with a group, ask the lead authority if you may give an initial talk about your proposed project to potential participants. At this meeting you can hand out information, explain the data collection process and answer questions.

e) All participants, whatever age, must have given their **informed consent before taking part**. This involves having their questions answered and understanding how the material they provide will be used.

Make sure people take part willingly:

- Provide accessible clear information to those who may be taking part.
- Avoid any requirement for participants to provide data when you first contact them (so as to give them time to reflect).
- Reassure all participants that their decision to share data (such as their flood experiences) will not affect their usual relationship with the school or group.

Important points about informed consent

- Provide accessible consent forms that are age appropriate.
- Participants over 16 years old can sign their own consent forms and do not need parental/carer consent. They may give informed consent should they reach 16 before the end of the project.
- If the participant is under 16 or a vulnerable adult, they and their parent/carer should be involved in the consent process. For children under 13 the parent/carer will usually be primary signatory with the child also signing their consent. Children over 13 are usually the primary signatory with the parent/carer signing their consent. These are ethical (not legal) processes that ensure that the child or young person, whatever age, has the right to refuse consent, even if their parent/carer consents.
- Consent includes giving permission for authorities to use and publish any 'data' involving them, which may be video or audio recordings, photographs or transcripts. Separating out these data on the forms means participants are able to consent to some but not all types of material being shared.
- All participants have the right to withdraw from the project. Children under the age of 16 have the right to refuse or withdraw from participation regardless of parental consent and without any persuasive action on the part of parent(s), teachers or other authorities.
- If a person withdraws, every effort must be made to delete their material but they should be advised that deleting their (anonymised) contribution to group discussions may not be possible. This information should be given to the participants as part of gaining their informed consent.

If you intend to work with children you may wish to consult Research with children in **The Research Ethics Guidebook** (Institute of Education, University of London): www.ethicsguidebook.ac.uk

Stage 2 - Data Collection

a) **Methods for data collection:** Choose methods that are appropriate and accessible for all participants and for the context in which you are working.

b) **Venues:** Choose a venue appropriate for your project. Alongside any possible DBS issues mentioned earlier, avoid lone working and attend to your own safety as well as that of participants. Ensure the venue space and surroundings are suitable e.g. holding a discussion in an open-plan office where others might overhear does not protect your participants and might affect the recording quality. These issues should also be considered in the setting up of post-flood drop in sessions.

c) **Supporting participants:** Set out a risk assessment, including an action plan should participants become distressed. Follow the guidelines which allow for breach of confidentiality should a child or adult disclose harm to themselves or others. Invite co-workers along so there is support during the sessions. Ensure that participants have access to means of support should they need them afterwards.

d) **Managing the data collected:** (1) the nature and type of data and (2) **recording devices, storage** and **archiving**.

Type of data: personal versus anonymised data

Data may include **text, audio or video recordings, photographs, artwork, internet or social media material**.

Data is considered either:

- **Identifiable**: this is data that includes personal data (names, contact details, age, gender, any other potentially identifiable details such as images stored as photographs or film or inputs on social media). All personal data should be destroyed once you have disseminated your findings.
- **Anonymised**: this is material with all personal data removed and **either**:
  - no potential identifiers, if text **or**
  - minimal identifiers, if images or audio. See below for guidance on anonymising visual data.

Anonymised data is **stored** for a stated time – typically 10 years after the end of the project. There are exceptions: oral history projects or data considered rare and unusual, or in the public interest (e.g. historical accounts, specific records of events etc.) may be **archived** in perpetuity.

Whatever the data type, **storage** must comply with the **General Data Protection Regulations** (GDPR, 2018). This replaces the Data Protection Act (1998) and has a particular focus on how personal data is managed.

Recording devices, storage and archiving

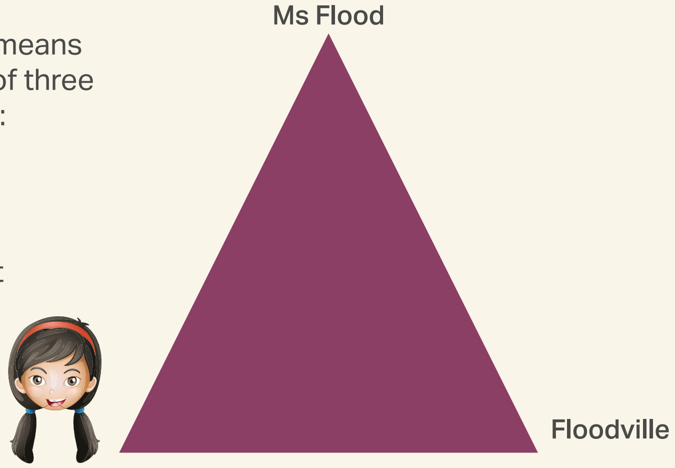
- Where possible, electronic data should be transferred to secure, encrypted storage and **anonymised** at the earliest opportunity following collection. Paper (hard) copy should be stored in a locked filing system in a locked office. Temporary secure encrypted storage includes portable devices:
  - encrypted recording devices
  - encrypted USB memory sticks
  - encrypted laptops
- Long term storage is recommended to be cloud-based or another secure institutional server or data repository
- **Personal data** must be stored separately from data that has been anonymised and should be deleted at the end of the project (this allows for authorities to send participants a summary of findings, invitations to feedback meetings etc.).
- If identifiable visual images are collected (photographs including people's faces, or project films etc.) it is advised that participants sign an additional consent or '**media release form**' (see example: www.lancaster.ac.uk/floodarchive/how-to-guide). This gives them the right to request the original image be removed from the data repository. Data used in publications or public films should be anonymised or follow the 'triangle of risk' and participants be aware that once in the public domain it will not be possible to remove.

Using the **'triangle of risk'** for visual data means making sure to use no more than two out of three possible identifiers e.g. on image captions:

1 Participant's name

2 Location

3 Image that would identify the participant (e.g. of their face or home)



Stage 3 - After Data Collection

a) After collecting the data, you may want to use it simply for publicity or as a record of the project. However, you may also want to **analyse** it to better understand people's experiences and perspectives and to inform future decision-making.

b) **Publishing data/dissemination**: it is important to share with participants how their data is used. Feedback groups or mutual learning events are recommended if the analysis may have an impact on practice and policy. Participants (and authorities) may want to use social media such as Twitter, Facebook or Instagram to post images from and reports of the project. So, it is important to set out your policy on both the choice of social media platform and how you manage these postings:

- Ethically, findings should follow the data management practice as above. Only use generalised anonymised text (use pseudonyms) in summaries, presentations and social media postings.
- Follow the 'triangle of risk' principle for visual images, including those posted on social media, to avoid identifiable images.
- It is recommended to have a specific custodian of social media accounts that authorities manage so images are sent to that custodian for posting. You may also request groups do not post up on other sites without checking with authorities (in practice this is more difficult as groups/schools will have their own policies and are often keen to post about involvement in projects). These basic points help to ensure that the policy for avoiding risk with project images is managed as closely as possible.

c) In **preparing reports and publications**, you should follow the same ethical practice of removing any information or combination of names, locations and images that could lead to identification of individuals.

Further information on the ethics of collecting data from people

Economic and Social Research Council Research Ethics www.esrc.ukri.org

British Sociological Association BSA Statement of Ethical Practice www.britsoc.co.uk

British Psychological Society BPS Code of Human Research Ethics (end edition, 2014) www.bps.org.uk

Flooding – a social impact archive is funded and managed by the Joint Environment Agency,
Defra, Natural Resources Wales and Welsh Government,
Flood and Coastal Erosion Risk Management Research and Development Programme.

www.lancaster.ac.uk/floodarchive