

Data Management Plan

Types of Data:

The source data for the project consists of 1) survey data from online and scanned paper questionnaires; 2) digital scans of documents collected (manuscripts, relevant newspaper and magazine articles; 3) video and audio recordings, including phone calls; 4) transcriptions of video and audio recordings and text message conversations; and 5) fieldnotes from observations.

Data and Meta-data standards

The audio data will be in .mp3 format, the video data will be in .mp4 file format, and the transcriptions are in F4/F5 format, compatible with Atlas.ti database software and .rtf format. As far as we know there are no accepted metadata standards yet for ethnographic video data. We have however, a robust system of metadata developed over the course of 10 years of handling video data in our past research projects, and these include date, time, place, pseudonyms of participants, and additional notes taken by ethnographers. These have been entered into the data files by assistants as they are uploaded, the meta-data themselves typically take the form of .rtf files that are downloadable from the Atlas.ti database software that we use to maintain the research project. These will be printed also as a physical artifact and stored in a locked cabinet.

Policies for access and sharing and provisions for appropriate protection/privacy

Within the constraints of our IRB agreements, we will make the data available on our websites, through a password protected portal. Following these constraints, we would anticipate making selected examples available as early as 18 months following the completion of the project, thus winter of 2018. Interested parties may apply to use it, and upon receiving agreement from the PI and co-PIs may apply for IRB approval. There are no current plans to charge for access.

We do anticipate ethical and privacy issues associated with its use. Because data will include videotape, audiotape, photographs, and documents, participants will be identifiable with respect to some of our data (via their images and their names on various documents). What follows are the procedures we will employ to protect participant confidentiality and privacy: All names on participants' work (e.g., professional development documents, lesson plans) will be replaced with participant identifiers. In cases of video and audio data, pseudonyms and other identifiers will be created. These identifiers will be codes that do not include any information that can be used to link back to participants. The link between names and participant identifiers will be kept separate from the data and stored in a locked file. Only the members of the research team will have access to this link. Field notes resulting from all observations, interviews, and focus groups will be kept in digital format (e.g., Microsoft Word, text, graphics), and kept on password-protected computers. The participant identifiers will replace any participant names (with the key kept separately in a locked cabinet). Photographs taken by researchers and participants and any participant written logs, lesson plans, etc. will also be kept in a locked office. Only the video, audio, photographs, and documents that participants consent to our using will be considered "data" and made available to the community (research and practitioner) at large. Audiotapes and videotapes will be transcribed and any references to participants will be removed or replaced with participant identifiers. Tapes will be stored in a locked file in a locked office and access will be limited to research co-investigators only. Researchers will sign a confidentiality agreement that states their agreement of non-disclosure of any information that

directly identifies participants. We will retain data indefinitely and potential research participants will agree to this as part of the formal consent process.

Policies and provisions for re-use, re-distribution The data will be restricted to research, teaching, and professional development purposes only. Other researchers, government district, personnel, and educational researchers are likely to be the main users for this dataset.

Plans for archiving and Preservation of access We store the data on the password protected GWU cloud/CITRIX server and it will also be backed up on a local password protected RAID/network drive. A record has been created for each recording file created that contains each piece of metadata associated with that file. In past research, we have developed FileMaker Pro databases to log all research events and the associated data (physical, digital, etc.) for each event. These databases sit on password protected computers and servers and ensure that data tracking, management, and retrieval is efficient. The original proposal, references, status update reports, IRB documents, research papers, and conference proposals and presentations will be stored indefinitely on this server and archived. Data collected in Washington DC in GW's password protected Citrix server and backed up with the local password protected RAID/network drive.