LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
PROF. DR. HELLA VON UNGER
INSTITUT FÜR SOZIOLOGIE
LEHRBEREICH QUALITATIVE METHODEN DER EMPIRISCHEN SOZIALFORSCHUNG

Data management in qualitative methods training

Handout for Students

This handout contains suggestions for handling qualitative data collected and analyzed by students as part of their methods training. What needs to be considered in order to enable responsible handling of these data? What role do research ethics and data protection issues play? These questions are the focus of the suggestions we have compiled here based on our experience at the Institute of Sociology at LMU Munich.

The handout is aimed at students and refers to qualitative data that are available in digital form. The handout by no means covers all questions and eventualitiesof qualitative data management. On the one hand, technical possibilities for digital communication, networking and data processing are constantly evolving, and data protection regulations and their interpretation are also changing. On the other hand, data management in qualitative research can basically only be planned in advance to a limited extent. The actual appropriate form of responsible data handling is usually worked out successively and together with the lecturers/project leaders in the research process. We would therefore like to encourage students to seek dialogue with the lecturers on these questions repeatedly. In doing so - so we hope - this guidance can offer orientation and suggestions. We are happy to receive suggestions for improving this handout (unger@lmu.de).

Content

1 General information on data security: Using LMU emails and infrastructure

For data protection reasons, please always use your LMU e-mail and the university's digital infrastructure.

If necessary, please turn off the forwarding function, which automatically forwards emails from your LMU email (@campus.lmu.de) to a private email address, for the duration of the qualitative research work.
Since qualitative research often involves working with sensitive data, the use of private e-mail accounts is not recommended. The access and storage conditions of commercial email providers (such as web.de, outlook, googlemail etc.), do not meet academic standards of data security and confidentiality. Therefore, please always use your LMU email.

Please store data in secure locations, i.e., on *password-protected* laptops, computers, and hard drives, as well as university online storage such as LMU Teams or Sync&Share (see below).

1.1 Collecting data yourself in qualitative methods training

At the Institute of Sociology at the LMU, qualitative methods training takes place in a variety of formats. In tutorials, seminars and research internships, you will have the opportunity to acquire practical research skills *hands-on*. In the process, you will also often collect and evaluate your own data.

Qualitative research thrives on the reflection and discussion of one's observations and interpretations. An exchange with other researchers (e.g., in the context of interpretation groups and research workshops) plays a central role. Therefore, you will usually work together in groups (2-4 persons) during the methods training.

In some courses, the groups each work with their own data corpus. In other seminars, everyone works together on one topic and the whole seminar accesses a common data corpus. In both cases, *data* are shared.

1.2 *Data sharing* via LMU teams

"LMU Teams" has proven itself as a technical infrastructure for secure *data sharing*, which guarantees a high level of security and data protection on the university's own servers and at the same time good accessibility of the data for teaching and research purposes.[1]

LMU teams are requested via a simple form[2]. Teams for the entire seminar are requested by the lecturers. However, students can also apply for their own teams for their working groups. To do so, enter "student team"[3] as the team form on the form "I would like to create an LMU team".

In order to use LMU Teams, it is necessary that your user ID is activated via the LMU portal.[4] Various folders (and subfolders) can then be created in the teams, e.g., for literature, slides, data and memos. The teams can also be used for discussions, chats, questions and appointments/calendar functions.

---

[1] At *LMU Teams there* are different types of teams: the "Virtual Seminar Room" is particularly suitable for courses; there are also "Project Groups" and "Student Teams", which can also be set up by students; http://www.hilfe.teams. uni-muenchen.de (accessed: 01. 02.2022).
[2] http://www.hilfe.teams.uni-muenchen.de/gruenden/antrag/index.html (accessed 01.02.2022).
[3] https://www.hilfe.teams.uni-muenchen.de/gruenden/registrierung/index.html (accessed: 01.02.2022)
[4] http://www.hilfe.teams.uni-muenchen.de/beitreten/kennung_freischalten/index.html (accessed: 01.02.2022)

The LRZ service "Sync & Share", which is available to all employees and students at Munich universities, has also proven its worth.

2 Confidentiality when handling the data

2.1 Confidentiality agreement (in the seminar)

A central principle in dealing with data is confidentiality. Please ask your lecturers if it is not entirely clear to you what this means in a specific case.

Many lecturers make verbal or also written agreements with students on the subject of "confidentiality". An example of a written confidentiality agreement can be found in the appendix). This agreement is made between lecturers and students - it is to be distinguished from a declaration of consent by the study participants (see below).

2.2 Contact details and field access

When planning field access, practical, data protection, research ethics and technical questions arise in the handling of the data. Contact data of (potential) study participants (e.g., names, addresses, telephone numbers, e-mail addresses) must be treated with special confidentiality, stored carefully (and separately from other data), and usually deleted after the end of the project. If further contact is planned (e.g., as part of a panel study), this should be clearly communicated at the beginning and explicit consent obtained from the participants (cf. 2.3).

For methodological and analytical reasons, it is also advisable to document field access well. If this is established via social networks, platforms, chats or e-mails, these interactions should also be saved as data and treated confidentially. Already here, it is essential to pay attention to the security of the communication channels. As mentioned, this includes using only your **university email**, deactivating forwarding functions to other, private emails, as well as considering encrypted communication channels if necessary (see 2.8 on encryption).

2.3 Informed consent

As a rule, the informed consent of participants is required for empirical social research. This can be obtained verbally or in writing (see our handout on study information and informed consent).

If participants' consent is obtained verbally, it is advisable to document this (e.g., in field notes, postscripts, or on audio recordings). Take time in the course - and ask - to clarify the procedure with the other students in your group and the instructors. Ask whether you should obtain consent in writing or verbally, and whether there is a template.

If participants' consent is obtained in writing, ask which form you should use if necessary - or whether you should develop one yourself. Also clarify where and how the signed consent forms will be stored - whether you will take care of this or whether the lecturers want

to store them centrally. Sample written consent forms can be found, for example, at RatSWD (2014), Helfferich (2009), and Audiotranscription[5].

There are justified exceptions to the rule of obtaining informed consent (e.g., field research in public places or analysis of documents freely available on the Internet).

2.4 Record conversations

Please make sure to use only professional recording equipment for audio recordings of interviews and group discussions (and the same applies to video recordings).

Audio recording equipment can be borrowed from the Institute of Sociology for three months with the payment of a deposit. [6]

We strongly advise against using private smartphones as recording devices. Although these now have powerful recording capabilities, private smartphones are often networked in many ways and there is a risk that the recordings will be uploaded (accidentally or automatically) to cloud services, for example, where they are no longer adequately protected but may be accessible to third parties - or even formally become the property of the providers.

Please delete the data completely from the recording device again (after transferring it to a safe storage location).
It is recommended that you delete the data on the recording device's stick while the stick is connected to the computer- and then check again on the display of the recording device whether the deletion has actually worked.

2.5 Preparing and naming data

In qualitative research, a wide variety of empirical material is collected, so that questions arise about the meaningful processing, naming, and securing of this data. Not all data can be digitally processed. In principle, it makes sense to agree on naming practices at an early stage in order to establish a designation system that is as uniform as possible. This facilitates data management and promotes an overview of the data corpus (cf. Tab. 1 for an example).

Data sort	Formula	Example
Field notes	FN_Name Student_Date/YYMMDD	FN_Rösch_180525
Audio files	INT_ID/Pseudonym_INT Date	INT_Lara_180530
Transcripts	TS_ID/Pseudonym_INT Date	TS_Lara_180530
Postscripts	PS_ID/Pseudonym_Date	PS_Lara_180530
Documents	Author/Org_Year_Title Keyword	DAH_2015_Annual Report
Newspaper article	Newspaper_Date_Title	SZ_180530_Roseanne Twitter

[5] A sample consent form for interviews that complies with the new EU Data Protection Regulation can be found at: https://www. audiotranskription.de/qualitative-interviews-DSGVO-compliant-recording-and-processing (accessed: 01.02.2022).
[6] https://www.soziologie.uni-muenchen.de/institut/it-service1/software_geraete_verleih1/index.html (Accessed: 01.02.2022)

Tab. 1 Example of the designation of selected data types *(Note on the legend: Field notes (FN) are named here after the authors; audio recordings of interviews (INT), on the other hand, are named after the code (ID) of the interviews and the pseudonym of the interview partners; the name of the postscripts (PS) also refers to the interviewee, and not to the interviewer and author).*

In the case of a shared, centrally managed data corpus containing interviews, it is advisable to jointly select a transcription style (with corresponding character legend) at an early stage and to apply this consistently.[7] The same applies to the preparation of video data.

2.6 Anonymize and pseudonymize data

In principle, data are anonymized as early as possible to protect the participants. Different anonymization strategies are used (cf. Saunders et al. 2015). Common is the pseudonymization of names (e.g., Lara instead of Birgit or Mr. Huber instead of Mr. Strubel). Other names (e.g., of organizations) as well as other information about people and places are also deleted, changed, or oversimplified (e.g., "Munich" can be oversimplified to "southern German city"; a "managing director" becomes an "employee in a managerial position", etc.). The purpose is to prevent the identification of the persons involved and to protect them. However, the nature of qualitative data is such that it can only be anonymized at the expense of its informative value, and it can basically never be entirely anonymized (unless it is completely redacted). "Insiders" can recognize people simply by how they speak and what they say. Therefore, formal anonymization is often not sufficient to rule out inferences about individuals. At the same time, we have to be careful not to delete or change too much in order to still be able to meaningfully evaluate our data.

Practical tips for anonymization:

- **The basic rule is *to* anonymize as little as possible, and as much as is necessary.** As little as possible to retain as much of the informative value as possible, but as much as is necessary in the sense that in the event of increased risks and foreseeable harm, stronger interventions may be required to protect the participants;

- Anonymization takes place in several steps: the raw material of the data is first anonymized (as sparingly as possible) during the preparation of the data; after the analysis, quoted excerpts from the material are anonymized more elaborately, if necessary, during the writing of the term papers or publications;

- In the **raw material,** therefore, anonymize rather cautiously at first (i.e., initially pseudonymize only personal names) in order to preserve references and details and thus the informative value of the data and to enable a meaningful interpretative analysis;

- In the course of the analysis, and especially in the case of **quotations in the term paper** (similar to research reports and publications), more elaborate anonymization is performed and based on the material a decision is made as to which further form of anonymization is appropriate. It is important to weigh which information must necessarily be preserved (at this point) to describe the context and enable understanding, and which information must be shortened, omitted, or oversimplified (or presented separately) to ensure sufficient protection, e.g., because the data are sensitive, the persons are particularly vulnerable, or the topics are controversial.

In a taught research project with refugees (von Unger 2017), for example, anonymization was very elaborate and comprehensive because the participants were very vulnerable in

[7] Cf. the notes on transcription in Dresing/Pehl at www.audiotranskription.de (accessed 01.02.2022).

social, legal, and economic terms due to their current situation and their refugee background. In other studies, however, less protection may be required because the individuals are less vulnerable or the data less sensitive.

Likewise, depending on the research interest and circumstances, new and different questions may arise (such as special regulations for the protection of minors). It is generally recommended to ask the lecturers in case of uncertainties and to exchange ideas in your group.

If translations are required, the translators and interpreters are also obligated to observe the guidelines regarding anonymization, confidentiality and the appropriate handling of the data.

2.7 Data sharing - for all types of data?

In the courses, data is shared among students and with lecturers. Lecturers should decide together with the students which data will be shared in the seminar. For example, **field notes** are not only very difficult and costly to anonymize, but can also be very personal and reveal a lot about the person of the researcher - therefore, the respective authors should help decide which data will (and which will not) be made available to the other students in the course.

Another question is whether audio files should be shared, as these are significantly more sensitive and even more difficult to anonymize, as voices can be recognized. We usually handle access to this type of data rather restrictively in our teaching unit. For example, in the above-mentioned research project with young refugee interviewees, we made the transcripts and postscripts of usable interviews available via an LMU team, but not the field notes or audio files. Field notes were discussed and sometimes read by each other in the groups, but were shared as complete raw data, if at all, only within small groups. Audio files of interviews (collected and transcribed in the first semester) were not made available (in the second semester) through the joint LMU team. In case audio files needed to be re-listened to, e.g., to touch up transcripts, we made the audio files accessible *ad personam* on institute-owned computers in a protected folder on the institute's server (on the CIP drive)[8].

Regarding the technical implementation of *data sharing* in the seminar, special attention is paid to the security of the data. As already mentioned, we advise using secure, university-owned infrastructure. In LMU Teams, access is limited to subscribed individuals. Documents can be uploaded, downloaded and stored on your own computers. If this is planned, the data documents should additionally be encrypted by means of a password so that they remain protected when downloaded to private computers (Word documents can also be encrypted). [9]

Lecturers usually require all the data collected or at least should have access to this data as supporting proof for students' graded assignments.

For courses with a **centralized** data corpus, they compile the data corpus based on student submissions, check the data for sufficient anonymization, for example, and adjust file designations and the like.

For taught research projects in which data management is carried out **decentrally** by several groups, and in which data sharing is limited to the members of these groups, it is

[8] To set up secure CIP drives, see the instructions provided by the IT Support of the Institute of Sociology: https://dienste.soziologie.uni-muenchen.de/faq-pmwiki/pmwiki.php?n=Main.InfosFuerLehrende (accessed: 01.02.2022)

[9] Note: However, password-protected data cannot be further used with all programs for data-based analysis - MAXQDA, for example, cannot open password-protected files.

worth discussing the mode of data storage and access. Please do not use external providers such as Dropbox, Google Drive, or similar providers, as the research data are not secure here. If you do not want to apply for a separate LMU team, switch to **LMU Sync & Share**[10] as another LMU service or to other options, which are encrypted with verifiable servers.

2.8 Encryption of data and communication

Files, folders, storage media and communication (e.g., emails or chats) can potentially be encrypted or password protected.

PDFs and Word documents can be password protected[11] via the software.

Entire folders can also be encrypted[12] as ZIP folders, i.e., as compressed folders. However, the password protection disappears as soon as the individual files are unpacked.

Storage media, e.g., USB sticks or hard disks, can also be encrypted. Drives can be protected[13], for example, using the Bitlocker program, which is integrated in Windows. Sensitive data are only stored and used on protected storage media.

Email communication can also be encrypted. Prerequisites for this are an email address that is accessible via POP3 or IMAP (LMU addresses are) and the use of an email client (such as Thunderbird).[14] For double security, LMU has a separate certification procedure that must be followed in order to communicate via LMU email addresses in encrypted form.[15]

Further Guidelines

- Ensure anonymization in the long term: As a rule, do not make qualitative raw data accessible to third parties, or only after thorough consideration and with the explicit consent of the participants, in order to protect the privacy of the participants and limit the chances of deciphering the anonymization; never publish the entire raw data, but only quote[16] excerpts;

- When submitting assignments that are to be graded, clarify whether, how and in what form the raw data are to be made available to the lecturers (e.g., not in the appendix, but separately via password-protected sticks, see below).

[10]Sync & Share works like other cloud services, e.g., Dropbox. After logging in, folders can be created and made available to certain people via the user ID. There is 50GB of storage available to everyone. In addition, there is a client for all operating systems, as well as an app for Apple and Android. People can be invited to the folder via their email address.

[11] The detailed instructions can be found under the FAQs of the IT Support of the Institute of Sociology https://dienste.soziologie.uni-muenchen.de/faq-pmwiki/pmwiki.php?n=Main.PDF-Passwortschutz (accessed: 01.02.2022)).

[12] When creating a ZIP folder with the program IZArc (e.g. via right click on a folder > Add to ZIP-File Archive) there is an option "Encryption". There select AES 256 bit and set a password).

[13] For example, right-clicking on the removable disk and selecting the "Enable Bitlocker" option can very quickly protect a USB stick.

[14] Online you can find a lot of instructions and tutorials about the encryption of emails, see for example https://netzpolitik.org/2013/anleitung-so-verschlusselt-ihr-eure-e-mails-mit-pgp/ (access: 01.02.2022).

[15] The exact instructions can be found under the FAQs of the IT Support of the Institute of Sociology https://dienste. soziologie.uni-muenchen.de/faq-pmwiki/pmwiki.php?n=Main.MailverschlSselung (accessed: 01. 02.2022)

[16] On the debate about digital archiving of qualitative data for (secondary) research purposes, see: https://www.ratswd.de/dl/RatSWD_WP_267.pdf (accessed: 01.02.2022).

3 After submission of the graded assignment

3.1 Deletion of the raw data

At the teaching and research unit of Qualitative Methods (Prof. von Unger), we advise against submitting qualitative raw data (e.g. field notes, transcripts) as an attachment when handing in graded assignments, since, as mentioned above, these data cannot be anonymized completely or only with disproportionate effort, and the long-term storage of graded assignments is beyond the control of the lecturers (graded assignments are archived centrally by the institute; BA and MA theses also by the examinations office). It is, however, possible to submit the raw data **separately,** e.g., on a memory stick, which is returned or destroyed when the graded assignment is done, the term paper is discussed, and the project is completed.

Please ask your lecturers how to proceed with the raw data.

At the official end of the project, the question arises as to the deletion or further use of the data. Here, corresponding data protection regulations must be observed. In the confidentiality agreement with the students, we usually specify a time for the deletion of private copies on the students' storage devices (e.g., at the end of the semester, on the submission date of the term paper or at the end of the taught research project). If students continue to use their data for writing a thesis, it is advisable to make a separate arrangement.[17]

3.2 Secondary analyses

You are interested in doing more - and want to pursue the research work further, e.g., in a BA or MA thesis?
Then contact a) the possible supervisor early on, and b) clarify with the lecturers of the course whether you may continue to use the data from the course, and if so, which and how. In principle, this is only possible after consultation. In doing so, not only the personal rights of the researched persons, but also those of the fellow students must be respected.

3.3 Notes on legal framework - GDPR

The EU-wide regulations on the General Data Protection Regulation (GDPR), which have been in force since May 25, 2018, also [18]affect data management in qualitative social research. What this means in practice is currently being clarified. We will elaborate more on this point in the next update of this handout.

In any case, it is recommended to **document** the **management of the data** during the entire process from data collection to data deletion. For taught research projects, it is also important which persons have access to the relevant data.

[17] For separate instructions on deleting data, see among others: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Daten-endgueltig-loeschen/daten-endgueltig-loeschen_node.html (access: 01.02.2022).
[18] https://www.datenschutz-grundverordnung.eu/ (accessed: 01.02.2022).

4 Literature and links

Berliner Methodentreffen (2007): Memorandum für eine fundierte Methodenausbildung in den Human- und Sozialwissenschaften. https://berliner-methodentreffen.de/weiteres-memorandum/ (accessed: 01.02.2022).

DGS and BDS (2017): Ethik-Kodex der Deutschen Gesellschaft für Soziologie (DGS) und des Berufsverbands Deutscher Soziologen (BDS). https://soziologie.de/dgs/ethik/ethik-kodex (accessed: 01.02.2022).

Helfferich, Cornelia (2009): Die Qualität qualitativer Daten. Manual für die Durchführung qualitativer Interviews. Wiesbaden: VS Verlag.

Hopf, Christel (2009): Forschungsethik und qualitative Forschung. In: Flick, Uwe; von Kardoff, Ernst; Steinke, Ines (Eds.): Qualitative Forschung. Ein Handbuch. Reinbek bei Hamburg: Rowohlt, pp.589-600.

RatSWD (2014): Datenschutzrechtliche Anforderungen bei der Generierung und Archivierung qualitativer Interviewdaten. Working Paper 238. Council for Social and Economic Data, Berlin. http://www.ratswd.de/dl/RatSWD_WP_238.pdf (accessed: 01.02.2022).

RatSWD (2015): Archivierung und Sekundärnutzung von Daten der qualitativen Sozialforschung. A statement by the RatSWD. Council for Social and Economic Data, Berlin. https://www.ratswd.de/dl/RatSWD_Output1_Qualidaten.pdf (accessed: 01.02.2022).

RatSWD (2016): Forschungsdatenmanagement in den Sozial-, Verhaltens- und Wirtschaftswissenschaften. Orientierungshilfen für die Beantragung und Begutachtung datengenerierender und datennutzender Forschungsprojekte. RatSWD Output 3 (5). Rat für Sozial- und Wirtschaftsdaten, Berlin. https://www.ratswd.de/dl/RatSWD_Output3_Forschungsdatenmanagement.pdf (accessed: 01.02.2022).

Schaar, Katrin (2017): Die informierte Einwilligung als Voraussetzung für die (Nach-) Nutzung von Forschungsdaten. RatSWD Working Paper 264. https://www.ratswd.de/dl/RatSWD_WP_264.pdf (accessed: 01.02.2022).

Saunders, Benjamin; Kitzinger, Jenny; Kitzinger, Celina (2015): Anonymising Interview Data: Challenging and compromise in practice. *Qualitative Research*, 15 (5), pp.616-632.

von Unger, Hella (2014a): Forschungsethik in der qualitativen Forschung: Grundsätze, Debatten und offene Fragen. In: von Unger, Hella; Narimani, Petra; M'Bayo, Rosaline (Eds.) Forschungsethik in der qualitativen Forschung: Reflexivität, Perspektiven, Positionen. Wiesbaden: Springer VS, pp.15-39.

von Unger, Hella (2014b): Forschungsethik in der Methodenlehre: Erfahrungen aus einem Soziologie-Seminar. In: von Unger, Hella; Narimani, Petra; M'Bayo, Rosaline (Eds.): Forschungsethik in der qualitativen Forschung: Reflexivität, Perspektiven, Positionen. Wiesbaden: Springer VS, pp.209-231.

von Unger, Hella (Ed.) (2017): Junge Geflüchtete, Bildung und Arbeitsmarkt. Ein Lehrforschungsprojekt. Munich: LMU Munich. http://nbn-resolving.de/urn:nbn:de:bvb:19-epub-41306-4 (accessed: 01.02.2022).

von Unger, Hella (2018): Forschungsethik, digitale Archivierung und biographische Interviews. In Lutz, Helma; Schiebel, Martina Schiebel; Tuider, Elisabeth (Eds.): Handbuch Biographieforschung. Wiesbaden: Springer VS, pp. 681-693.

von Unger, Hella; Narimani, Petra; M'Bayo, Rosaline (Eds.) (2014): Forschungsethik in der qualitativen Forschung. Reflexivität, Perspektiven, Positionen. Wiesbaden: Springer VS.

Further links and references can be found on the website of the teaching and research area qualitative methods of empirical social research: http://www.qualitative-sozialforschung.soziologie.uni-muenchen.de under "Resources".

Acknowledgement

Staff members of the teaching and research unit of Qualitative Methods in Empirical Social Research at the Institute of Sociology at LMU Munich have contributed significantly to this handout (or a predecessor version). These include Yvonne Berger, Gözde Celik, Oskar Fischer, Holger Knothe, Dimitra Kostimpas, Anne Götz, Anna Huber, Dennis Odukoya, Hans Pongratz, Viktoria Rösch, Penelope Scott and Jana Türk. Many thanks!

Status: 01.02.2022

5 Appendix

5.1 Example confidentiality agreement with students

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

INSTITUT FÜR SOZIOLOGIE
PROF. DR. HELLA VON UNGER
LEHRBEREICH FÜR QUALITATIVE METHODEN DER EMPIRISCHEN SOZIALFORSCHUNG

Vertraulichkeitsvereinbarung

Name:	Matrikel-Nr.:	Dozent/in: Prof. Dr. Hella von Unger

Hiermit verpflichte ich mich, alle im Rahmen der Veranstaltung „Junge Geflüchtete, Bildung und Arbeitsmarkt" (Master Forschungspraktikum, 6 SWS, 15232, WiSe 2016/2017) erhobenen und zur Verfügung gestellten Daten streng vertraulich zu behandeln.

Das heißt:

- Ich verwende personenbezogene Daten und Informationen ausschließlich in anonymisierter Form, so dass kein Rückschluss auf die Identität der Teilnehmenden möglich ist (entsprechend dem Bundesdatenschutzgesetz und dem Bayrischen Datenschutzgesetz; s.u.).
- Ich verwahre die Daten an einem sicheren und passwortgeschützten Ort.
- Ich übergebe alle Daten (z.B. Audioaufzeichnungen, anonymisierte Transkripte und Feldnotizen) mit meiner Hausarbeit dem Lehrbereich für Qualitative Methoden (Prof. von Unger).
- Ich verwende zur Sicherung/Lagerung der Daten keine Online-Dienste wie Dropbox, Google Drive oder sonstige Clouds (mit Ausnahme LRZ Sync+Share und LMU TEAMS)
- Ich vernichte private Kopien der Daten (digital und ausgedruckt) zum Ende des Wintersemesters (23.4.2017).
- Ich verwende die Daten nur nach Rücksprache und mit ausdrücklicher Genehmigung von Prof. von Unger für weitere wissenschaftliche Arbeiten (z.B. Master-Arbeiten).
- Ich werde keine die Daten betreffenden Informationen schriftlich oder mündlich an dritte Personen, die nicht an der Lehrveranstaltung teilnehmen, weitergeben oder zugänglich machen.
- Ich gehe achtsam mit den Daten im öffentlichen Raum um (z.B. Gespräche in der U-Bahn)

Ich habe den Ethik-Kodex der Deutschen Gesellschaft für Soziologie (DGS) zur Kenntnis genommen (http://www.soziologie.de/de/die-dgs/ethik-kommission/ethik-kodex.html).
Bei Fragen wende ich mich an eine/n Mitarbeiter/in des Lehrbereichs für qualitative Methoden der empirischen Sozialforschung oder an Prof. von Unger (unger@lmu.de).

Ort, Datum: Unterschrift:

5.2 Check-list for data management in qualitative methodology

In summary, we suggest that the following points be considered in data management:

- ✓ Use campus email (and turn off automatic forwarding)?
- ✓ Use secure digital infrastructure for *data sharing* (e.g. LMU teams).
- ✓ Questions about confidentiality clarified?
- ✓ Questions about study information, contact information, and field access discussed?
- ✓ Informed consent (of participants) - verbal or written?
- ✓ Use professional recording equipment
- ✓ All digital research communication via LMU campus emails only.
- ✓ Discuss anonymization strategies
- ✓ Password protection of data (encryption)
- ✓ Encrypt storage locations (e.g. external hard disks or USB sticks)
- ✓ Set up secure, university-owned cloud services for group work.
- ✓ Clarify preparation (e.g., designation, transcription legend) of data.
- ✓ Clarify submission, retention, and deletion of raw data (e.g., delete recordings on recording devices before returning them).
- ✓ Discuss possibilities for further use and reuse of the data (e.g. for publications or qualification work).
- ✓ Document data management