Research in the Digital Space: Things to consider

1. Introduction

1.1 Queen's University is committed to ensuring research is undertaken with integrity. This high level guidance has been developed to inform researchers about key legal and ethical considerations when undertaking research in digital spaces, either through the use of platforms to conduct research, or the use of platforms to access data to be researched. It cannot be prescriptive for every situation, and it should be read in conjunction with several supporting sources. To ensure all appropriate ethical considerations are made, consult the QUB Policy on the Ethical Approval of Research. Consideration should be given to the policies that govern the use of I.T, data and information security.

1.2 The **terms that govern legal use** of data are outlined in the **Terms and Conditions** of particular platforms. It is important that researchers review and understand these T&Cs to ensure compliance and take the appropriate steps to mitigate ethical issues.

1.3 It is an individual researcher's responsibility to ensure they are aware of and adhere to Data Protection legislation, notably the Data Protection Act 2018. Researchers are responsible for compliance with data protection requirements, and this must be considered when platforms to undertake research are selected. This may mean that individuals need to be flexible around their choice of platform, depending on the nature of the research.

1.4 When planning your research and determining which platform is to be used, the ethical issues posed by both the platform and the actual research should be carefully considered. These ethical issues will only be evident through the careful review of the platform's terms and conditions of use. It is also important to consider data management, in terms of safety and transparency for both participant and researcher. Whether the researcher is using online platforms to carry out research or collecting data from online platforms such as social media, blogs reviews etc, the project requires ethical review in the same manner as face-to-face research. This is because the data being collected belongs to a human participant.

1.5 This high level guidance is designed to support researchers in their understanding of the intricacies presented in digital research. The document does not address AI and/or Chatbot generated information, rather researchers should consider any internal guidance produced by the University and/or professional bodies/learned societies that may be relevant to their discipline/research.

2. Planning your research

2.1 At the outset of any research project, consideration must be given to the research data:

- why it is being collected,
- what is being collected,
- how it is to be collected and used,
- who will use it/store it, and
- how it will be made public in the interests of research transparency, if possible.

All such considerations should form part of the research data management plan for the research. A data protection impact assessment (DPIA) may be required depending on the nature of your research. A DPIA allows you to assess and mitigate risks

associated with the information processing, and support compliance with data protection legislation. Please contact the Library's Open Research Team for further support with DMPs and the Information Compliance Unit for further support with DPIAs.

2.2 As part of **data management** considerations it is vital that researchers **review and consider the key legal and ethical considerations** about the digital platform they intend to use. The platforms Terms and Conditions should be reviewed so there is full understanding of current requirements and/or uses. Researchers should consider what is recorded during the activity, including any chat discussions, conversations or other. This could potentially hold personal/sensitive data and should be reviewed and stored or deleted, in line with your agreed retention and deletion timeframes. In addition, consideration should be given to what the platform/third parties itself is recording during the research activity.

2.3 Various digital platforms provide facilities. The University's preference has been MS Teams, however, it is recognised that this may not always be possible or the most suitable, depending on your participants. No matter what platform you use you must consider **functionality** required, for example around attendance lists, recording of the sessions and the capture of chat functions. This must be considered in advance and also that of the potential behaviours of those participating (e.g. recording sessions without permission). If using MS Teams to conduct or disseminate research and you require IS support on these matters, contact Information Services and request ticket support to view the session's statistics.

2.4 If the digital activity is captured in any written notes, or recorded in any form, personal[1]/private[2] data must be stored as appropriate on secure, encrypted QUB devices.

2.5 Before sharing any files or other material that contain personal data you must be satisfied that the individual/organisation has a lawful basis to receive the information. Data should only be shared if part of a collaboration agreement or using a data transfer agreement which will clearly define the data protection requirements that must be adhered to by the other organisation.

2.6 When sharing data, ensure that any transfers are secure and completed via appropriate mechanisms i.e. end to end encryption. Transfers between QUB researchers in a research team is covered by end-to-end encryption when QUB e-mail server is used. Personal data must not be sent unencrypted via email, chat etc.

2.7 Further support or guidance in relation to the data privacy implications of using MS Teams in a research setting can be obtained from the Information Compliance Team: info.compliance@qub.ac.uk. The advice provided by them will be specific to the nature of your research, therefore it is important you clearly describe your research in your request to them.

2.8 The Open Research Team can provide support and guidance on Funder requirements; Copyright; Uploading Datasets to Pure and supporting researchers in applying for Active Data Storage.

[1] Personal data is information held about a particular person which is sensitive to them and helps to identify them.

[2] Private data is data that can be traced back to an individual, often private data is not made available to the general public.

3. Research in the digital space

3.1 *Digital environments*: **Countries govern** their data, software, technology in a variety of ways. It is important that researchers know their collaborator and the **legal requirements of the country they are based and/or come from**. There may be a requirement by your collaborator to undertake some internet surveillance for the state, or openly report research to the state. In turn, this may breach what is ethically planned and/or data protection legislation, it may compromise the security of the research data being collected. Therefore, it is critical that researchers are aware of and have undertaken open-source due diligence on their partners prior to commencing their work.

Researchers should consider:

- 3.1.1 the categories of data that the chosen platform gathers from its users, the rights it gives third-parties, and taking steps to keep researchers, participants and their data secure as much as is within their capacity;
- 3.1.2 utilizing their particular mechanisms to develop an ethical stance towards participants and their data e.g. markers of access[3] or privacy, 'gatekeepers' (i.e. persons who control access to online platforms), user expectations.
- 3.1.3 the potential risks associated with collecting and analysing social media data. Researchers collecting and analysing social media data must familiarize themselves and abide by the privacy restrictions, user settings, and legal requirements of the social media platforms they intend to use. These policies vary across different social media platforms and the geographical location of the host server. Care must also be taken to remember that these evolve over time so it may be necessary to undertake due diligence on the country or parent company.
- 3.1.4 whether it is appropriate to use personal social media accounts for conducting online recruitment. Doing so can reveal private information about the researcher and may also share participant's details with others, who are not part of the study. Where a personal account is to be used for research purposes, this should be clearly justified to the Research Ethics Committee and explanations given regarding the protection of participants

3.2 *Ground rules*: Researchers should make participants aware of their obligations to each other when hosting research using on-line or in-person group approaches to ensure there is clear understanding as to what they can and cannot do or say during the event. As a University researcher, consideration and application of the appropriate policies (Data protection policy; Data Security Policy and Policy on Recording of Educational Materials) needs to be adhered to. The researcher might want to consider and provide ground rules on the following:

a) to record the session. This includes audio and/or visual recording and screenshots, image captures, chat functions.
b) to document or share information outside the session.
c) respectful use of the chat functions and break-out rooms.

4. Researcher/Participant interaction

[3] Markers of access are dependent on the owner/administrator of the platform being used so whether the group is open to all or closed so only those who have subscribed can comment. This is managed in different ways by the various platforms.

4.1 As research using a digital platform involves collecting data from human participant(s), either directly or indirectly, it is crucial that the ethical aspects of the research are robustly considered. It is necessary to consider the following:

- Whether the data being collected relates to personal or private data, as defined earlier,
- What the user settings are for the platform
- Are there any legal requirements, in particular, could the data be repurposed by the platform being used?
- Are there any other practices by the platform that require taking cognisance of?
- The plans you have for the data in terms of openness and transparency, the reporting of the research, for example will verbatim quotations be captured in publications, how data will be managed, maintained and/or retained and for how long?

In considering these various elements you will consider how the rights of the potential research participants are affected. The Association of Internet Researchers provide Ethical Guidelines which are a useful resource.

4.2 *The definition of a research participant* in online or digital settings is more diverse and requires careful consideration by the researcher; for example:

4.2.1 user profiles may not accurately reflect the people behind them (e.g. avatars, organisational accounts, 'public' figures);

4.2.2 beyond primary participants, digital data may also involve others e.g. in the same network or discussion.

4.3 *Public and private:* even when digital data exists in the 'public domain[4]', there may be legal and ethical considerations to consider before using it in academic research:

4.3.1 Researchers seeking to conduct research-related activities in online spaces need to be mindful of whether the space is private or public. This determination will affect the way in which the researcher should proceed with respect to research-related activities. Consideration should be given as to whether the data is truly 'publicly available' without a login or social media account, specific permissions, paywall etc. Could redacted metadata and/or summarised data in aggregate form be sought?

4.3.2 However, the boundary between private and public is not always clear. The QUB Policy on the Ethical Approval of Research highlights that there is a more blurred distinction and users are not always fully aware of how their data is employed. Researchers should not assume that 'public' data can be freely used for research with no ethical implications.

4.3.3 Different platforms' in-built mechanisms for distinguishing between public and private may be of use to the researcher in ethical decision-making. For instance, data arising from a public user account or page is ostensibly more public than that generated in 'closed' groups, private discussions or by private user accounts.

4.3.4 *Private spaces*: Researchers wishing to conduct research-related activities in private spaces – i.e., those that require special permissions to be granted in order to enter – should seek permission from the relevant body (e.g., the creator, or manager of the online space/group before conducting any research-related activities.

4.4 *Public spaces*: Researchers seeking to conduct research-related activities in online spaces which are ostensibly public i.e. where there are no barriers or special entry

[4] Data that is in the public domain is available to the public as a whole, especially through not being subject to copyright or other legal restrictions.

permissions – must be respectful of already existing participants in the online space. This entails that (a) the researcher provides existing participants with an opportunity to disclose any discomfort or objection to the researcher's presence, and (b) that all research-related activities be as minimally disruptive as possible. If participants disclose discomfort or object to the researcher's presence, the researcher must not conduct any research-related activities in that space. Researchers must ensure that any research-related activity (e.g. recruitment, observation, seeking consent) does not hinder normal group activity. Researchers need to be particularly sensitive of the fact that conducting research-related activities in online spaces may be viewed in a negative light

4.5 *Recruitment:* There are unique challenges with respect to recruiting participants using digital platforms which include the wording of participant information sheets and consent forms. It is important that researchers consider whether a privacy policy/statement is required to govern your research, what information the participant needs to have, how you have managed their receipt and understanding of information relating to the research and most importantly how consent is to be captured. Other key issues to be planned as part of the research include:

4.5.1 *How you will make a call to research participants*: Researchers should carefully manage the dissemination of online recruitment announcements, for example, does the call come from a personal email or a work email account. Research conducted on behalf of Queen's should always come from a Queen's account.

4.5.2 *Do potential research participants merit inclusion:* Researchers should ensure that research participants meet the inclusion criteria necessary for participation in the research project(s). This is particularly important as often emails/announcements can be spread widely, and it is necessary to ensure that you engage with those persons who should be included in the research.

4.5.3 *Ethical Review*: In seeking the review and approval of a Research Ethics Committee for digital research it is necessary to provide details of recruitment documents and processes to be used and managed, especially if recruitment is via social media. The areas relating to public/private spaces, methodology of recruitment, how consent is to be managed, the need for/use of privacy statements etc must all be articulated and presented for consideration.

4.6 *Informed consent and the right to withdraw*: the most important principle in human participant research, informed consent, is also relevant in digital research. Informed consent entails those potential participants be fully informed about the research, before giving their consent to take part:

4.6.1 informed consent should generally be attained from participants when gathering qualitative or verbatim data,

4.6.2 participants in digital research should be fully informed about how their data will be collected by the researcher on chosen platform, it may well be necessary to provide details if the platform itself collects data.

4.6.3 It is also important to detail how long the data process will take and how long data will be retained for. Critical in this context is the use of the platform to collect the data and then the possible use of a different platform for uploading/sharing the research.

4.6.4 When gaining consent, it is important that consideration is given to the final publication of the data and/or onward sharing. Data may be aggregated which helps with protecting anonymity or it may be quantitative in nature. However, qualitative data, in particular, the use of direct quotations may result in the identification of a participant.

4.6.5 'Implied consent' involves the assumption that - because users agreed to a platform's terms of service - consent for their data to be used by third parties (inc. researchers) is thereby implied; this approach may not be ethical in all cases; For example, secondary analysis of anonymous data compared to manual data scraping or fully automated data scraping from online sources. As detailed in section 1.3 it is also the responsibility of researchers to evidence fair use of data from online sources and where 'implied consent' is being used. For research using online methods to collect qualitative data participants should be provided the privacy notice/statement of third parties.

4.6.6 'the right to withdraw' is complicated by the enduring nature of digital data; steps should be taken by researchers to uphold participants' rights to withdraw and to be forgotten (e.g. by checking for data deleted by participants following data collection);

4.6.7 the Data Protection Act 2018 also supports users' right 'to be forgotten', also known as the 'right to erasure', which has implications for the retention and storage of research data which researchers must be cognisant of.

4.7 *Anonymity*: It is impossible to guarantee anonymity to research participants, rather you can endeavour to commit to keeping their involvement in the research confidential. It is important to consider how this can be achieved:

4.7.1 In group activities online, participants' names may be visible to other users. Participants should be informed before giving consent whether pseudonyms may be used or that anonymity can only be imposed after online data collection.

4.7.2 Even if data is anonymised retrospectively, consideration needs to be given to the fact that participants' identities may still be traceable online, depending on the nature of the data.

4.7.3 Where a researcher has concerns relating to safeguarding, they have a duty to take appropriate action in accordance with the University's Safeguarding Policy. An escalation process should be identified prior to the research commencing so there is clarity as to how safeguarding matters are to be dealt.

4.7.4 Where research participants are being sought using social media platforms, there is increased risk of exposure to the researcher. It is important that this risk is considered and documented so there is a clear path of action identified in the event the researcher feels threatened. If researchers feel at risk of harm, they should raise this with their Head of School/Centre Director, the University's Designated Safeguarding Officer (DSO) or Deputy Safeguarding Officer, as applicable.

Glossary

Data scraping	The extraction of data from web sources, or use of software code to extract data from websites which is prepared for processing, analysis or presentation.
Collaborators	Researchers working on a similar research project.
Partners	Groups or persons who are stakeholders in the research being undertaken