University of Surrey Ethics Guidance for Social Media Research

Introduction

This guidance is designed to assist researchers in navigating the ethical considerations of social media (SM) research. It acknowledges the unique ethical challenges of social media research while supporting researchers to undertake such research. Researchers are encouraged to consult their disciplinary guidelines when drafting ethics applications to ensure alignment with broader academic norms.

It focuses on helping researchers identify different levels and types of risk associated with:

- **Participants** (privacy, consent, vulnerability)
- **Data** (personal vs. non-personal, public vs. private, scale of data, sensitivity of data)
- **Platforms** (Terms of Service, changing rules)
- **Researchers** (personal safety and wellbeing, legal obligations)

It also outlines specific considerations for student projects involving SM research.

1. Key principles

1.1. **Respect for autonomy and privacy:** Researchers must respect the autonomy of social media users by considering their privacy expectations regarding the content they create, share and consume online, as well as the platforms, groups or other networked spaces they may be a member of or participate in, either actively or passively. Social media content and participation, even when seemingly public, is unlikely to have been intended for research purposes nor these purposes anticipated by users.

1.2. **Informed consent**: Consent remains a critical ethical requirement, though its consideration and enactment within SM research is nuanced. Researchers should consider platform Terms of Service (ToS), the public/private nature of data, and seek explicit consent where feasible, especially from vulnerable groups or individuals.

1.3. **Risk-based approach**: Research on social media should follow a risk-based framework, evaluating the potential risks for participants, data and researchers. This assessment should guide decisions on consent, anonymisation and use/publication of data.

1.4. **Situational ethics**: Digital research scenarios vary, and no single set of rules can cover all situations. Ethical decision-making should be context-driven, flexible and reflexive, allowing for reasoned cases where standard protocols cannot be applied, with researchers responsible for considering and developing these cases.

2. Risk identification and mitigation

2.1. Risk to participants

- **Data sensitivity**: Consider the sensitivity of the data being used, especially personal or identifying information. For example, public comments (e.g., on 'newsfeeds' or open groups) might still carry an expectation of privacy.
- **Public vs. private**: Evaluate whether social media data is truly public. Even data shared in spaces that are potentially accessible may be contextually private (e.g., closed groups or platforms requiring logins) whereby the intended and expected audience for the data is limited in scope.
- **Vulnerable participants**: Extra care is required when engaging with vulnerable groups, such as those discussing sensitive topics (e.g., self-harm, political oppression) or whose identification (be that online or offline) may put them at risk.

2.3. Risk to data

- **Legal requirements:** Researchers must, as a matter of course, follow platform ToS and avoid unauthorised data scraping. If using tools to collect large datasets, ensure compliance with both ToS and legal frameworks (e.g., GDPR). Given that social media operates across across multiple jurisdictions, and the legal framework governing data use can vary dramatically by country, there may be international privacy laws, platform-specific rules, or local regulations that affect the legal use of data. Researchers must assess jurisdictional risk, particularly when using global platforms where users and data may come from multiple legal contexts. This includes understanding how international laws affect data collection, storage, and sharing.
- **Data collection**: The ethical use of social media data requires researchers to navigate the platform's ToS and the rules of specific online spaces. Even when data appears publicly available, platforms and online communities may have their own boundaries regarding data collection, sharing and use. Researchers must respect these boundaries, secure consent from platform authorities or group moderators where necessary, and should recognise that some platforms or spaces may reject research access entirely. However, there may be occasions where reasoned cases can be made for violating ToS or requirements for consent, with guidance outlined below.
- **Data security and anonymisation**: Personal data must be securely stored, pseudonymised or anonymised where possible. Public figures may not require anonymisation, but ordinary users often expect privacy, with further guidance, including regarding reasoned cases for non-anonymisation, outlined below.

- **Distinctions between passive and active data collection**: Researchers should carefully consider the degree of interaction and whether passive or active collection changes the risk profile of their project. The more direct the engagement, the higher the need for consent and ethical scrutiny:
    - **Passive collection**: This refers to gathering data from publicly available posts without interaction, which may seem low risk. However, even passive observation can violate users' expectations of privacy, especially if posts are taken out of their intended context (e.g., quoting posts from a small support group).
    - **Active collection**: Engaging directly with users, through surveys, interviews, or participation in groups, introduces additional ethical complexities, such as the need for explicit consent, managing participant expectations and addressing power imbalances.
- **Bot activity, trolling and misinformation:** Researchers must consider the authenticity of the data they are collecting and assess whether it reflects real user behaviour or manipulative content. It may be necessary to conduct a verifiability assessment to ensure the authenticity of the data, especially when researching politically sensitive topics or controversial online spaces where bots and trolls are common.

2.3. Risk to Researchers

- **Personal safety**: Researchers working in online environments where harmful content is prevalent (e.g., extremist groups) should consider personal safety measures, such as limiting exposure and securing institutional support. It may also be necessary to share and agree protocols with relevant departments, e.g., IT Services, for accessing material/groups/sites that would ordinarily be prohibited.
- **Legal and institutional risk**: Researchers must ensure compliance with legal frameworks, including GDPR, especially regarding data collection, retention and publication.

3. Navigating consent and anonymity

- **Platform-specific context**: The norms and rules of engagement on different social media platforms often shape how users communicate and present themselves. For instance, what is considered public on one platform may feel personal or private to users depending on the platform's features and audience. Researchers must respect the platform's context and understand that users' online behaviours may not translate into consent for research. Data used out of context can misrepresent the persona the user intended to convey, including if misunderstood or stripped of context in the analysis.
- **Diverse expectations of publicity and privacy**: While some users actively construct a public-facing persona, fully intending their content to be seen, shared and potentially analysed (e.g., influencers, activists, public figures), others may only expect visibility within specific

community contexts or platform boundaries. The expectations around privacy, autonomy and consent will vary depending on how public the content is intended to be. Researchers must navigate this range of expectations, recognising that public visibility does not automatically equate to consent for research use. High-profile accounts may imply consent for wider use, while ordinary users may still expect privacy even in semi-public or searchable spaces.

- **Disparities in user agency and platform power:** Platforms often hold significant power over user data, and users may not fully understand the implications of sharing data under specific platform terms. There is a risk that users may not have genuine agency over their online data, even when it is publicly accessible. Reearchers should take into account power imbalances between users and platforms, as well as between researchers and participants. This includes scrutinising whether users were fully aware of the platform's data practices and how these impact their consent

- **Implied consent**: Some research may rely on implied consent. For example, some individuals may wish to maintain the integrity of their statements and receive attribution for their contributions. This is especially relevant for public figures, activists, influencers or users who engage in public discourse with the intent of being recognised. In such cases, anonymising or altering their data for the sake of privacy protection could violate their personal or professional interests and distort the original meaning of their statements. Researchers may wish to consider consulting the user, where feasible, to clarify their preferences regarding attribution and/or should maintaining the integrity of direct quotes or contributions to avoid altering the original message in ways that might misrepresent the user's intent. Researchers should clearly explain and justify their decisions regarding anonymisation, consultation and attribution.

- **Contextual consent**: Consent in social media research extends beyond individual users to the groups, spaces, and platforms in which those users interact. Online communities often function with distinct norms and expectations regarding privacy, membership and interaction. Researchers must consider not only whether individual users have consented to the use of their data but also whether the community or platform (e.g., moderators, gatekeepers) has given tacit or explicit consent. For closed groups or spaces where access is restricted, gaining approval from gatekeepers or adhering to community guidelines important. Reasoned cases may be made if gaining approval is not to occur (see below).

- **Longitudinal research**: If social media research involves longitudinal or historical data, there may be risks related to the evolving privacy norms or expectations over time. What was once considered public or innocuous may later be viewed as private or sensitive. Researchers should factor in the potential evolution of user expectations and the platform's practices, particularly if there is a significant time lag between data collection and publication.

- **Anonymisation techniques**: Where consent is not feasible or where there is otherwise a reasoned case for not seeking content, anonymisation and aggregation of data can help protect participant identity. However, anonymised data should still be scrutinised to ensure individuals cannot be indirectly identified. It is important to consider the identification of individuals online and the risks they may face if identified in online environments (e.g., exclusion from an online community, online harassment, etc.) and risks related to identification offline. It may not be sufficient just to mitigate the risks and consequences of offline identification if the data to be processed and published may also lead to a person being identified online.
- **Altering data**: If proposing to anonymise the data through altering of users' content, researchers should ensure that they are not misrepresenting users' intentions or unduly distorting the content.

5. Adaptive and dynamic ethical review

- **Continuous ethical review**: Ethical considerations do not end with the initial ethics approval. Researchers must continually assess risks and compliance. This includes if platform ToS change during the course of the research. Platforms frequently update their ToS, which can affect research practices mid-project. A platform's ToS may change in ways that limit data collection, enforce stricter rules around data use or introduce new privacy protections.
- **Reasoned cases**: Researchers should be prepared to present reasoned cases for any deviations from standard practices (e.g., not seeking explicit consent). This includes making arguments for public interest, participant protection or platform-specific issues. Disciplinary norms and existing/previous practice can be cited as part of reasoned cases.

For example:

- **Breach of platform terms and covert research**: In certain cases, breaching platform ToS may be ethically justified, particularly where the public interest or the need to expose harmful practices overrides the obligation to follow platform rules. This is especially pertinent in areas of covert research within criminology, sociology or studies of marginalised or hard-to-reach communities. For example, research on extremist groups, organised crime or online hate speech may require a covert approach to avoid jeopardising the research or the safety of participants and researchers. Likewise, while platforms often dictate data access and usage through ToS, researchers may argue that platform-imposed restrictions should not unduly limit research, especially when it concerns public interest issues like political manipulation, misinformation or criminal activities.
- However, researchers should weigh the potential harm that could arise from breaching platform policies against the public benefit of the research. Ethical oversight should include a reasoned case, outlining the justification for such actions, how risks will be mitigated and why covert research is the only viable approach. Specifically, researchers should ensure that:

- The research cannot be conducted through other means (e.g., openly or with informed consent).
- The potential benefits of the research outweigh the risks of conducting it covertly or breaching ToS.
- There are clear safeguards to protect both participants and researchers from harm.
- Ethical approval includes a detailed risk assessment and justification for covert methods.

6. Researcher and participant safety

- **Researcher protection**: The University supports researchers engaging with sensitive or harmful content for research purposes. Researchers should take breaks, use University-provided resources (e.g., institutional emails for recruitment), and ensure secure work environments, alongside any other health, safety and wellbeing protocols relevant to research in these domains.
- **Participant safety**: Ensure that research does not place participants at risk, particularly in contexts where online activities may expose them to harm or legal repercussions (e.g., research in politically sensitive areas).

Supporting undergraduate and postgraduate researchers

Supervisors play a crucial role in guiding students through ethical decision-making. Supervisors should work closely with students to help them navigate ethical reviews, design robust research proposals, and understand the implications of their methods (e.g., data scraping, participant observation, or interacting with users on social platforms). It is also advisable to ensure that students, particularly undergraduates, are provided with dedicated modules or workshops on digital ethics, platform-specific risks and consent in online spaces.

- **Streamlined ethics review for low-risk studies**: Many undergraduate and some postgraduate projects may involve low-risk research, such as analysing publicly available data from high-profile social media accounts. A simplified ethics process may be possible for such projects (e.g., pre-approval via Standard Study Protocols). For higher-risk research, such as studies involving sensitive topics, vulnerable groups or private online communities, students are required to submit more detailed ethics applications with comprehensive risk assessments.
- **Support for managing sensitive or harmful content**: Students may not be adequately prepared for exposure to harmful or distressing content (e.g., extremism, self-harm forums or hate speech) and may require additional support if undertaking research on these topics. Students and supervisors should assess the potential emotional impact of the project and include mitigation strategies in their ethics applications.

- **Researcher safety**: Students working with high-risk content, such as extremist groups or controversial political issues, should outline how they will protect their personal safety, including how they will anonymise their own online presence, use secure university accounts and avoid prolonged exposure to harmful material.
- **Platform ToS and data collection**: Students need to familiarise themselves with applicable legal and ethical implications of their proposed data collection methods (e.g., on the use of APIs, limitations of scraping tools, or data retention) to help avoid breaches of ToS and other legal issues. Students need to adhere to GDPR and other data protection regulations, particularly regarding identifiable personal data. They should be supported in designing projects that minimise the risk of breaching data protection laws and taught how to handle data securely and anonymise it where appropriate.
- **Anonymisation and consent:** Students may struggle with balancing anonymisation and maintaining the integrity of social media data. Student applications should clearly outline how they will apply anonymisation without distorting the research outcomes or breaching user expectations, with supervisors potentially involved for cross-checking anonymisation.
- **Consent and interaction**: Students must understand the nuances of consent in online research, particularly in closed or semi-public online spaces. Supervisors should help students navigate when and how to seek consent from participants, gatekeepers or platforms, especially if their research involves direct interaction with users, with consent procedures clearly outlined in ethics applications.
- **Critical reflexivity in student research**: Students should adopt a **reflexive approach** to their research and evaluate their ethical decisions and the potential impact on participants. This can be integrated into their risk assessments, regarding anticipated risks and mitigation strategies.