



Guidance on the Ethical Use of Social Media in Research

1. Principles and Scope

This guidance should be used to help researchers who are using social media platforms to collect data or recruit participants for their research. It is expected that all students discuss the use of social media with their supervisors before beginning their research. Considerations around social media should always be explicitly detailed within the study's ethics application.

Social media research can comprise of quantitative, qualitative or mixed methods approaches. It typically involves human participants, whether that is actively (through interactions and participation, such as posting on social media platforms or speaking to users online) or passively (through observation, following pages and/or hashtags). Any use of social media should be the most appropriate method to use to answer the research questions, as stated by the [Government Social Research report](#).

Researchers should be guided by core principles when designing, implementing, analysing or disseminating social media research, as set out by governing bodies, such as the British Psychological Association (BPS), UK Research Integrity Office and Association of Internet Researchers (AoIR):

- Respect for the autonomy, privacy and dignity of individuals and communities, considering:
 - Public/private distinction
 - Valid consent
 - Confidentiality
 - Anonymity
 - Deception
 - Withdrawal
 - Copyright
- Scientific Integrity
- Social Responsibility
- Maximising benefits and minimising harm, considering:
 - Maximising the benefits of the research
 - Minimising harm to participants
 - Minimising harm to researchers

Emerging new technologies used by or via social media platforms, such as artificial intelligence and computer scripts (i.e. 'bots'), may present further ethical concerns so researchers should ensure they are aware of the latest guidance around the ethical use of AI in research throughout the lifecycle of the study including at the design, data gathering, data analysis, and dissemination stages.

'Contextual and reflexive' judgement is required for ethical consideration around research carried out online, rather than fixed rules as emphasised by [The Association of Internet Research](#), and it must consider the broad implications. There is no one-size-fits-all approach, and researchers are expected to use social media responsibly and transparently throughout the

lifecycle of the research project. From a GDPR perspective, all processing of personal data, regardless of origin, must protect the rights and freedoms of the individuals, reinforcing the ethical considerations around privacy. This applies irrespective of whether social media users have posted content within the public domain (see Section 2); a dataset such as this should never be considered “fair game” for scraping or analysis and researchers should consider the content they are analysing as deriving from ‘human participants’.

Given the rapid change in online platforms and activity, there are many ‘grey’ areas in social media research. Student researchers should discuss their use of social media with their supervisors, and all researchers should discuss with their LREC’s if they need advice on a specific project or matter. All research projects using social media require institutional ethical approval as per the University Research Ethics Policy.

2. Public vs Private data (incl. secondary data considerations)

Researchers must not assume that data from social media platforms are appropriate for analysis, simply because the content is accessible. The BPS and AoIR highlight the importance of distinguishing between public and private online environments and emphasise that ethical obligations depend on the context.

The [BPS Code of Human Research Ethics](#) (2021) states that unless consent has been sought, **observation of public content (e.g. behaviours, thoughts, attitudes etc.) needs to take place only in public situations** where those observed would expect to be observed by strangers (for example a blog like WordPress or online news article where the author is clearly named). It is not always easy to determine which online spaces people may expect to be observed or who they expect to be observed by.

Researchers should always consider the perception and intention of the user, as per the [BPS guidance](#), when there is a level of ambiguity concerning if data is public or not, and if there are any potentially damaging effects from using their data. Best practice would be to contact a group moderator or administrator for advice on these issues (for example when taking data from a Facebook or Reddit group).

Researchers should be aware and consider the relationship between platform and users, particularly considering that users may not fully understand the implications of sharing their data on certain social media platforms. Researchers should consider that many users of social media will not have read the platforms’ data practices before registering and so may not be aware of any consent for sharing they have agreed to. See section 6 for more information on platform terms of usage.

Researchers should always check before writing up their research that any direct quotations still exist as publicly available and haven’t been made private since the researcher first compiled their dataset.

3. Informed Consent (incl. withdrawal)

It is expected that consent be sought where participants are being recruited for a research study rather than being observed, where new data is being produced or where private data is being used. This may not always be possible or practical when using social media data. If in doubt about seeking consent, please speak to your supervisor (if a student), or LREC.

The terms and conditions of the platform being used may include permissions to publish datasets or users agreeing to the use of their data for research. However, researchers should consider whether their research project meets the reasonable expectations of the platform users for the use of their data for research. For example, researchers do not need permission to analyse Reddit content, but Reddit expects to be notified if a researcher then plans to publish data using their content.

The most appropriate and ethical way to contact users must be considered by researchers when informed consent is required from individuals. This can sometimes be agreed by a site moderator as 'gatekeeper'. Researchers should always remember that they are a representative of Leeds Beckett University when contacting others over the Internet for the purposes of their research.

There may be circumstances where it is safer and/or more ethically appropriate for the researcher to not seek consent. For example, contacting a group who share their extreme racial views may not welcome being studied. Furthermore, there may be instances where the revelation of researcher status would be highly problematic or risky to the researcher. In these cases, it may be safer for the researcher to not announce their presence. Please consult your LREC if you have specific concerns about this and justify your decision making within your ethics application.

It may be justified that gaining valid consent is not required if there is likely to be no perception and/or expectation of privacy from the original user, (see section 6 on platform terms of use) or where scientific value and/or research validity considerations are deemed to justify undisclosed observations. Where consent is not sought, ensuring data remains confidential (through anonymity etc.) is even more critical.

Implied consent may be relied upon in some research, particularly those involving public figures, or influences, where it appears to be obvious that individuals wish to be attributed to their statements and content. In such cases, it may be against their personal/professional interests to anonymise or alter their data for the sake of privacy. In this case, researchers should attempt to consult the user as far as is feasible to clarify their preferences and consent.

Participants should be informed of their rights to withdraw from participating in research when they are asked for consent. Any request to withdraw from studies should be complied with within a reasonable timeframe. Researchers should recognise and make clear to participants that once data has been aggregated, it may not be possible to identify, withdraw and remove individual data. Withdrawal procedures should be robust and made as clear as possible.

4. Personal data – anonymity and confidentiality (incl. legal considerations)

The collection of unnecessary personal data should be avoided, in accordance with UK GDPR, even if it may not be possible to guarantee that no personal data will be collected. It may be necessary to remove any personal data after collection.

Every effort should be made to protect the identity of participants in research particularly where informed consent has not been obtained. Anonymisation and aggregation of data can help protect the identity of participants, however researchers should scrutinise datasets to ensure that individuals cannot be identified through direct or indirect identifiers such as contextual information or combinations of data points. Researchers should recognise that most social media platforms require a user to register with personal data (e.g., email address, username, date of birth and/or image) to create an account or profile.

There can be no guarantee of full anonymity with social media research, but it may be possible to trace content back to the source which could have ethical implications for the individual/community being discussed, particularly if they are vulnerable or identify as a marginalised group. It may be necessary to replace identifying information (e.g. usernames) or redact any identifying information. Where this may be the case, please consider a scenario where removing an author's field may go against platform terms and conditions. For example, Twitter's terms of use state that the individual username must be displayed with the text of the tweet which in some circumstances may compromise an individual's safety or wellbeing.

Research with anonymised data could still cause harm to a group of participants, for example by discrimination or stigmatisation of entire sets of populations. This relates directly to the principle of minimising harm to participants. Researchers should consider whether participants may disagree with their interpretation and whether their interpretation of the data might marginalise an individual or group further.

Social media data, as with other research, requires the researcher to **consider how the data will be stored, shared and archived/destroyed**. Potentially identifiable social media data are subject to general LBU ethical requirements, data management guidelines and GDPR. All data considerations should be made explicit in the data management section of an ethics application or within the data management plan for staff researchers were required.

Researchers should also familiarise themselves with any potential issues relating to copyright on posts/images they want to reproduce. It may be possible to use content from copyrighted sources such as social media posts for non-commercial research under the government [‘exemptions to copyright’](#). This is provided that use does not financially impact the copyright holder or infringe on the copyright holder's rights. For any use of copyrighted work, you must ensure there is sufficient acknowledgement to the copyright holder.

5. Protecting participants

Researchers should consider how they will deal with ‘ethically important moments’ that may arise during their research and how they plan to respond to these. For example, in the case of conducting primary research, researchers may need to consider how they would respond to a person online who has said that they are planning to harm themselves or another person, or to

disclosure of harm related to a person under 16. Where a potential safeguarding risk is raised and a researcher is engaging in an active manner (e.g. online interviewing), researchers have a duty to inform participants that this disclosure may result in a breach of confidentiality. This risk can be minimised by asking participants in the information sheet to refrain from straying outside the topic being discussed. In the case of observing secondary data generated from social media (e.g., TikTok comments), researchers may still encounter a safeguarding or extremist (PREVENT-related) disclosure in the public domain. In this instance, whether historical or current, researchers should liaise with their nominated safeguarding lead and the Information Governance team, who will make the decision about whether to forward this information to authorities. Any concerns, whether conducting primary or secondary data research, should be discussed with a supervisor (if the researcher is a student) or a nominated safeguarding lead and the Information Governance team (if staff).

Researchers need to be aware that **the level of risk or vulnerability of participants is much more difficult to monitor or assess in social media research**. For example, there are likely to be fewer contextual and interpersonal cues that would otherwise help a researcher to identify distress, risk, or diminished capacity. Researchers should be particularly mindful that despite the platform's terms and conditions, it can be difficult to know the age of social media users, and so the requirement to obtain parent/guardian consent may not always be clear. Researchers should bear in mind that these 'vulnerable' social media users may not fully understand the consequences of their online activity.

As in all research environments, particular care needs to be taken when working with and taking consent from individuals or groups who are particularly vulnerable to coercion.

Where research involves particularly socially sensitive or high-risk topics, researchers should carefully consider whether social media is an appropriate method of data collection or whether the research could be conducted more ethically offline. This should also be considered if a researcher is unfamiliar with a particular platform or does not use social media themselves. Face-to-face or other offline approaches can provide greater control over participant recruitment, enable researchers to ensure that participants have received and understood key information relevant to informed consent (including the limits of confidentiality), and allow closer monitoring of disclosures made during the research process. Student researchers must only conduct primary or secondary data studies that have been approved by their subject lead. In this instance, a dissertation or proposal module leader should be able to advise based on what students have been trained to conduct. These considerations are especially important when the age of participants cannot be easily verified and/or the research concerns sensitive or potentially distressing topics, including but not limited to:

- Self-harm and suicidal ideation
- Violence and abuse, including sexual, physical, and emotional abuse

Researchers should consider that whilst their research itself may not cause any harm, unintended consequences of being included in a research study may inadvertently cause harm. This is particularly the case when looking at vulnerable or marginalised groups or sensitive topics, for example highlighting specific private forums for certain groups may bring unwanted attention from unwelcome users.

6. Platform – Terms of Usage and data authenticity

It is the responsibility of the researcher to consider and understand the terms of usage for any social media platform they are using for their research project and briefly outline a platform's data usage policy in their ethics application. Supervisors (in the case of students) and LRECs should not be expected to know or verify this when reviewing an application. Researchers are therefore encouraged to upload the platform's policy in the Documents section of Worktribe, especially if working with data that requires de-identification. It is worth noting that social media platforms regularly change their 'terms and conditions' (may also be referred to as 'community guidelines'), so researchers should always check for the most current versions.

Researchers should consider the conventions and norms of a specific social media platform, particularly if users would expect to be observed or not. For example, users who post openly on X would expect others to see their posts, whereas users posting in a private forum would not expect others to see or use their content. Researchers are encouraged to cite relevant codes of conduct or guidance to support their analysis of data if informed consent has not been sought (e.g., [BPS Ethics guidelines for internet-mediated research](#))

There are certain cases (as discussed in Section 5) where it may be ethically justified to breach a platform's terms of usage. For example, when it is in the public interest to expose harmful practice in areas such as extremism, safeguarding, organised crime, political manipulation or misinformation. This should be adequately justified in any ethical application for the study.

Researchers should consider the authenticity of their social media data and assess the extent to which their content reflects the activity of genuine users rather than automated or bot accounts. Where relevant, researchers should take reasonable steps to carry out a proportionate review of the authenticity of accounts and content, including looking at account verification status, profile information, posting frequency, engagement patterns, account creation data, follower relationships and any indicators of automated behaviour. This is particularly important in research areas where bots, coordinated activity or misinformation are known to be commonplace, such as political spheres.

Ownership of 'public' content on social media sites (photos, videos, chats etc.) remain with the service provider (the platform) and not with the author/user. Whilst it is not deemed practical or necessary to gain explicit permission for use from website owners/platforms, this is something researchers should keep in mind and content should always be de-identified wherever possible (e.g., removing a username from an image).

Researchers should consider the ethical issues associated with the use of algorithms when using social media platforms, particularly when they are using their own personal accounts. Where personal accounts have been used to collect social media data, researchers should reflect on how the platform algorithms may have shaped the data collected by prioritising certain content whilst excluding other content. Additionally, researchers should carefully consider the ethical implications of using algorithm-derived information to make

inferences about individuals or groups, particularly those who may be vulnerable, marginalised or at greater risk of harm.

7. Researcher responsibility, conduct and safety

Researchers should reflect at the beginning of their study if they are able and willing to identify themselves as a researcher on social media when conducting data collection. This should be possible in most cases but there may be instances where the researcher's identity is unknown to participants.

Covert research may involve participants not knowing they are part of a study at all, whereas deceptive research may involve participants believing the intention of the study is different from the real intention. Both are commonplace in social media research but researchers should consider the rationale and reasoning for this and how mitigations for any ethical risks will be managed. This should be explicitly discussed in the study's ethics application.

In most cases, it is best practice to avoid lurking on social media, meaning that researchers should be open about their presence and clearly communicate to other users the purpose and limits of any data they are collecting. This may include contacting gatekeepers or site moderators of an online page (e.g., Facebook) and/or posting a message on a forum of when a researcher is starting and ending their research.

Researchers must ensure they are protecting themselves when contacting others online. As the [AoIR Risky Research Report](#) emphasises, ethical use of social media involves protecting the researcher as well as the participants. Researchers should, where possible, avoid using personal contact details and disclosing any personal details such as addresses, phone numbers or email addresses. This is particularly necessary when contacting individuals or organisations that are known or suspected to be involved in harassment, threatening or hateful behaviour (e.g. far right supremacist, extreme racial groups etc.). The AoIR Risky Research Report highlights that social media research can expose researchers to harms including harassment, doxxing and reputational attacks. Researchers should therefore consider appropriate measures to protect their safety, wellbeing and privacy such as checking privacy controls on social media accounts and other public information available online about themselves. The University would expect that students have received sufficient training throughout their taught or research degree to conduct sensitive online research. Before starting any research in these areas, researchers should liaise with their respective module leader, supervisor or LREC.

Researchers should be aware that social media research increases the likelihood of exposure to sensitive or distressing content compared with more traditional research methods. There is also an increased risk of researchers encountering data that indicates a clear safeguarding risk (e.g. a confession relating to abuse of a minor, whether historical or not). This is becoming increasingly prevalent as the use of social media grows and becomes more embedded in everyday life, with exposure to sensitive, graphic and distressing content becoming increasingly commonplace online.

The university is supportive of researchers engaging with sensitive or harmful content for research purposes where social responsibility and scientific integrity can be clearly justified and referenced in an ethics application, however researchers are encouraged to be proactive

about their safety and wellbeing. Researchers engaged in these areas of research should be in frequent contact with their supervisors or line managers and should be aware of the wellbeing resources the university has available. It may also be necessary to share and agree protocols with the IT department, legal and/or Information Governance in circumstances where accessing or engaging with certain materials or groups would ordinarily be prohibited or limited.

It is generally expected that students and staff should use their university staff email address for any research that is affiliated with the university. Separate social media accounts should not be created unless this can be fully justified and approved in an ethics application. Researchers should consider the ethical implications of using personal social media accounts to gather data and of creating new or fictitious profiles purely for the purpose of gathering data. The line between openness/legitimacy and protecting the researcher is important to consider here. Researchers may be putting themselves at increased risk, for example by becoming subject to unwanted/uninvited contact by users that they are observing. A good example of this includes researching dating sites. It may also violate platforms' terms and conditions to create a fake profile for the purpose of research. If the latter applies, then researchers must not proceed. Again, the University would expect that student researchers have accessed sufficiently training on the implications of conducting such research where a fake profile is considered necessary.

8. Further Information and Relevant Documents

- British Psychological Society, [*Ethics Guidelines for Internet-Mediated Research*](#) (2021)
- British Psychological Society, [*BPS Code of Human Research Ethics*](#), (2021)
- Association of Internet Researchers, [*Internet Research Ethics \(IRE\) 3.0*](#). (2024)
- Association of Internet Researchers, [*Risky Research: An AoIR Guide to Researcher Protection and Safety*](#) (2025)
- Association of Internet Researchers, [*AoIR Ethics Panel 2: Platform Challenges*](#) (2021)
- UK Research Integrity Office, [*Ethical Issues in Research Using Social Media*](#).
- UKRI, [*Internet Mediated Research*](#).
- Gov.uk, [*Exceptions to Copyright*](#) (2021)
- University of Surrey, [*Ethics Guidance for Social Media Research*](#) (2024)
- London School of Economics, [*Using Data from the Internet and Social Media in Research: Ethics and Consent*](#). (2026)
- University of Edinburgh. [*Social Media Research Ethical Guidance for Researchers*](#). (2021)
- University of Bath. [*Research Using Social Media and Other Online Data*](#).
- University of the West of Scotland, [*Copyright and Licensing: Copyright and Social Media*](#)
- Government Social Research, [*Using social media for research: an introduction*](#). (2016)
- Wilkinson, D. and Thelwall, M., [*Researching Personal Information on the Public Web: Methods and Ethics*](#). (2011)
- Townsend, L. and Wallace, C., *Social Media Research: A guide to ethics* (2018).
- Paris Smith, [*Fake Social Media Accounts: Legal and Ethical Issues*](#). (2021)
- Elovici, Y., Fire, M., Herzberg, A. & Shulman, H., [*Ethical Considerations when Employing fake identities in online social networks for research*](#). (2014)
- Hine, C., [*Virtual Ethnography*](#). (2000)

9. Contributors

Charlotte McMahon, Research Ethics and Integrity Manager,
Nova Deighton Smith, Senior Lecturer, School of Humanities and Social Sciences,
Lauren Smith, Senior Lecturer, School of Humanities and Social Sciences,
Ellie Clement, Open Research Services Manager,
Jon Dart, Senior Lecturer, Carnegie School of Sport,
Darren Nixon, Senior Lecturer, School of Humanities and Social Sciences,