# Social Media and CCTV-Guidelines for use in research

This guidance should be used by researchers who are planning on using any social media platform (e.g. Facebook, Twitter, Instagram, Tik Tok, YouTube, etc) for either recruitment purposes or for the purpose of gathering and analysing user data. If your study involves one of these scenarios, please refer to the relevant section of this guidance for any specific considerations. If your study involves both of these scenarios then please read through all the guidance. Please note that because the landscape of social media platforms is continually changing it is not possible to issue platform specific guidance for all or even most platforms. These guidelines should therefore be interpreted with the specific platform(s) used in mind.

This guidance also covers the use of CCTV for the purposes of gathering and analysing user data. If this applies to your study you should read through the specific requirements and expectations for accessing and using this type of data for research purposes.

# Using social media platforms to recruit participants for your research study

## Advertising for research participants

- Researchers should not use their personal social media accounts to contact potential research participants but should instead explore the following options for advertising.
    - Set up and use a study specific account/page/group, being sure that the account name/page/group clearly indicates that it is for research purposes.
    - If the account is used exclusively for professional (e.g. networking) purposes, it can be used to post/share an advertisement provided that the researcher does not directly message their list of contacts with requests to participate in the research.
- If setting up a study-specific social media account/page/group, researchers should be clear about their intentions and specifically mention that any interactions with the research account/page/group including (but not limited to) posts to the account page, shares, and direct messages will be used for research purposes.
    - The accounts should also include a disclaimer or hashtag that indicates it is used for research purposes by the University of Manchester (or the named sponsor of the research).

## Gaining consent from participants

- When contacting potential participants via social media, researchers should always inform them of how they obtained their details, just as they would if they found their contact details on a publicly available website such as StaffNet.
- Researchers should ensure the recruitment for their study is targeted at public profiles, pages or groups. Specific individuals should not be targeted unless this can be adequately justified based on the research topic.
- If seeking to recruit via closed, private or restricted profiles, groups or forums the researcher must first seek permission of the moderator or owner for access.
    - Once permission is obtained to 'join' or access the profile, group or forum the researcher must post a message/advertisement visible to all users of the group outlining the research being conducted and the time period for participant recruitment.
    - The message/advertisement should also contain a hyperlink to the full participant information sheet as well as to the University's Privacy Notice for Research.
    - If a significant number[1] of users object to the researcher's presence the researcher must withdraw.
- Further communication with potential participants who indicate initial willingness to participate should take place on a one-to-one basis (using e-mail, private messaging etc) or move to a private forum/group with the researcher named as an administrator.

## How to ensure participants have the right to withdraw/correct their data

- When gaining consent, researchers must, unless data collection is anonymous, establish a process for participants to be able to withdraw or rectify any of their data used as part of the study or request a copy of the data and information used as part of the study, and participants should be informed about this process within the PIS.

## Ethical approval

- You should use the University's Ethics Decision tool in order to determine if ethical approval is required for your research project.

[1] As the exact number of the members of the group may not be known, it is not possible to provide an exact number for what would be deemed 'significant'. Therefore, researchers must consider this issue on a case-by-case basis and if any objection to their presence is made, make a reasonable determination as to whether they need to withdraw.

# Using social media platforms to gather/download/obtain information from or about users (with or without consent)

## Important considerations when accessing social media data from users

- The use of application programme interfaces (APIs) for data collection is standard across most platforms. However, researchers should take care when utilising these interfaces as accuracy depends largely on the query structure and programmes that are built by the researcher. In addition they cannot give complete assurance unwanted content will not be collected.
- The Terms and Conditions of social media platforms often prohibit collecting or harvesting personal data, even when the information is publicly available (See Appendix 1).
- Researchers should also consider whether using the data has potential negative implications for individuals due to the legislation/politics of particular countries (e.g. the Twitter and Facebook blocking in China).
- Social media data, even if publicly available, often contains the personal preferences, histories, and opinions that users are sharing with close personal friends and acquaintances.
    - Even if this information is in the public domain, it is not necessarily intended to be used by individuals who are merely 'followers' and not personal contacts.
    - There are numerous instances when users have been upset to find that what they thought were private conversations appear in other contexts.
    - Researchers should consider the specific context in which the information was posted, (e.g. was it posted many years ago, as some blog and twitter posts are intended to be an intervention in a public discourse at the time of posting).
    - Researchers should consider the time that has elapsed since the information was posted and whether any sensitivity of the posted content is likely to have decreased or increased.
    - These considerations should form part of the justification for how the data will be handled in the project. The ethics committee will take these considerations into account when reviewing the proposed strategy for data handling.

## Respecting the rights of social media users

- Researchers need to carefully consider what they will do if a user deletes a message/post/tweet or their entire account/page/group, if/how they will monitor this and whether this is classed as a participant 'withdrawing' from the study.
- To do this, researchers need to first distinguish between information that is gathered as part of a large-scale scraping exercise (e.g. combing twitter for 1000 tweets with a specific hashtag)

versus information that is obtained by embedding oneself in a private group/forum over a prolonged period of time to gather information.

  - For large scale scraping exercises, it may not be possible to identify data which has been removed by the user as researchers may not be actively monitoring for changes. In this case, it's important to anonymise the data as much as possible to reduce the risk of identification and possible distress to users who may come across the use of their data which has since been deleted.
  - For data gathered with the consent/knowledge of users, researchers need to remove user's data from their study if the user deletes this data from their social media platform unless consent is obtained to retain this data for research purposes.

- Researchers should consider the scope of information they are gathering and this should be proportionate and in line with the purpose/desired outcome of the research and therefore use tools/data which have the least intrusive impact on the user.
  - Additional considerations should be given to the timeframes of collecting the information and when information will become irrelevant/redundant.

## Publication of data: ensuring confidentiality and anonymity

- When used for research purposes, information should be anonymised to protect the confidentiality of individuals.
  - If this is not possible ethical approval must be sought
- If using publicly available photos or videos, researchers need to familiarise themselves with any applicable copyrights.
- Researchers should consider the traceability of a verbatim quote through search engines and how this will potentially breach a user's privacy and/or cause harm by way of embarrassment or reputational damage.
  - To avoid this potential, researchers should use paraphrasing[2] unless explicit consent from the user is obtained, or the user is a public figure (e.g. prominent politician, celebrity etc).
  - Researchers should also consider their own safety if publishing something contentious as participants might recognise themselves in quotes in the publication.

## When is it acceptable to use information available from social media without the consent of participants?

- Information in the public domain, including usernames, tweets, bios, posts or profiles, ***can*** be used for research purposes via techniques such as data mining without the explicit consent of users as long as all of the following are true. The data are:
  - publicly available
  - permitted to be collected under the terms and conditions of the specific social media platform being utilised (see Appendix 1)

[2] This would be classed as anonymising providing this is done to a sufficient standard as to make the paraphrase untraceable in a search engine.

- not likely to be from vulnerable or dependant groups, including children or young people[3]
- Or the data were clearly intended to form part of a public discourse when published, and there is no reason to believe that they are now considered personally sensitive by the original author(s).

- However, the research **may still require ethical approval.**

## When does research involving the use of social media data NOT require ethical review?

- All of the following must be true. Data are/will be:
  - Publicly available[4]
  - Non-sensitive[5]
  - Not involving vulnerable or dependant groups (including children/young people)
  - Anonymised[6]
  - Used in accordance with the terms and conditions of the specific social media platform (see Appendix 1 for more information)

## When does research involving social media require ethical review?

- Ethical approval will be required if **any** of the following are true:
  - Data are sensitive, confidential, restricted or private (e.g. data about mental health experiences/conditions, political opinions, religious beliefs, criminal offences, sexual orientation)
  - Data from private individuals (not including public figures, politicians, celebrities, etc) are identifiable and cannot be anonymised.
  - Data has a risk[7] of uncovering potential disclosure of criminal activity.
  - Data are from individuals considered to be vulnerable or dependant [including children or young people]
  - The project involves developing or using methods for re-identifying de-identified data.

[3] Researchers need to consider how they verify whether the data being obtained is from an adult, child under the age of 16 or a potentially vulnerable person. If they are unable to verify this information (e.g. because the platform does not provide the information), the study will require ethical approval.

[4] This refers to data that are available to the world at large and not just made available to a closed or otherwise restricted membership group.

[5] This is contextually dependent as what is considered sensitive in one context with one group of participants may not be considered sensitive in a different context with a different group of participants. Therefore, it is important that you consider this carefully for each research project you undertake.

[6] This refers to the data being anonymised at the point of collection/receipt/download. In this context, the term anonymised means that a piece of information would not be easily identifiable if published on its own. It would be advisable to perform a reverse Google search as that is likely to safeguard the researcher in the long run and protect the writer of the information being used from exposure or exploitation.

[7] As all research carries some form of risk, this is asking you to consider whether any such risks are merely hypothetical or real. If a real and probable risk exists that you will uncovering information that you would be required to disclose to the authorities, the study will require ethical review.

## Approval by full UREC review is required for any the following studies:

- Data are being collected from private[8] profiles, pages, groups or forums.
- Data being collected are confidential or personally sensitive.
- Data being collected may lead to data subjects experiencing negative effects on their personal, social, or economic well-being or significant levels of distress.
- Data may have a risk of uncovering potential disclosure of criminal activity.
- Data may be collected from data subjects considered to be vulnerable or dependant.
- You are actively researching topics that are likely to elicit responses from children and young people under the age of 16 years (i.e. the impact of gaming on school performance or topics in relation to children's television programmes/music/etc).

## Approval by the Division/School Committee or by the Proportionate UREC Committee is permitted for the following studies:

- Data DO NOT fall into any of the categories listed above.
- Data are being collected ONLY from public profiles, pages, groups or forums.

[8] This refers to the settings of profiles, pages or groups for specific social media platforms which restricts viewing access.

# CCTV -Guidelines for use in research

## When does research involving CCTV NOT require ethical review?

- Footage is publicly available without the need to obtain explicit permission from the organisation collecting it.
- Footage does **NOT** include sensitive/contentious activities or events (i.e. antisocial behaviour, protests, car accidents, etc).
- Footage will be fully anonymised/de-identified to protect the confidentiality of those involved.

**Important note: Even if the study does not require ethical approval it will require approval from the Information Governance Office. Please see section entitled Information about CCTV for more information on this requirement.**

## When does research involving CCTV require ethical review?

Ethical approval will be required for any study using CCTV footage if:

- The footage is obtained directly from the organisation collecting it.
- The footage will involve sensitive/contentious activities or events.
- The footage cannot be fully anonymised/de-identified[i].

## Information about CCTV

- Some CCTV footage is publicly available. However, it shows individuals going about their daily lives who have not agreed to be filmed for research purposes. They may not even know that they are being filmed.
- Some would therefore argue that individuals have a right to ensure any footage of them recorded in this way is kept private unless disclosure is absolutely necessary (e.g. reporting criminal activity or missing person's cases).
- Researchers should carefully consider this point if wanting to use CCTV footage for research purposes.
- As CCTV is highly intrusive in terms of people's rights and freedoms, researchers considering projects which will access this footage must contact the Information Governance Office (email: information.governance@manchester.ac.uk) as a data protection impact assessment will be required and only granted under exceptional and justified circumstances.

[i] In specific and exceptional cases, the ethics committee will permit the use of CCTV footage which is not fully anonymised/de-identified if it involves a highly public figure such as a celebrity, politician, etc. However, an adequate justification must be provided for cases such as this and include what measures you will take to protect the confidentiality of these individuals.

# Appendix 1: Terms and Conditions

## Adherence to terms and conditions

**Any research use of social information must adhere to the legal terms and conditions of the particular service. See below for direct links to the terms and conditions of some popular services:**

Please note that reading the terms once might not be sufficient as they are subject to repeated and rapid change.

- https://twitter.com/en/tos
- https://www.facebook.com/terms.php
- https://help.instagram.com/581066165581870
- https://www.tiktok.com/legal/terms-of-use?lang=en
- https://www.flickr.com/help/terms
- https://www.tumblr.com/policy/en/terms-of-service
- https://www.linkedin.com/legal/user-agreement
- https://about.pinterest.com/en/terms-service
- https://www.youtube.com/static?gl=GB&template=terms

# Appendix 2: Further Reading

A comprehensive resource that covers the ethical implications of involving people in research via social media can be found here: http://www.invo.org.uk/wp-content/uploads/2014/11/9982-Social-Media-Guide-WEB.pdf and a sensible US guideline for internet research here: http://aoir.org/ethics/

Additional resources can be found in Townsend & Wallace.