# INTERNET-BASED RESEARCH (IBR)

## CONTENTS

1. SCOPE OF THIS GUIDANCE ............................................................................................ 2
2. PUBLIC/PRIVATE ONLINE SPACE AND ETHICAL CONCERNS ...................................... 3
   2.1 Twitter ................................................................................................................. 3
   2.2 Facebook and Similar Social Media Networking Services .................................. 4
   2.3 Message Boards/Chat Rooms ............................................................................... 4
   2.4 Mobile Internet Connections ............................................................................... 4
   2.5 Deception ........................................................................................................... 4
   2.6 Dark Web Studies ............................................................................................ 5
   2.7 Deepfakes .......................................................................................................... 5
3. CONSENT ISSUES ..................................................................................................... 6
   3.1 Informed Consent in Social Media Research ..................................................... 6
   3.2 Implied Consent and Informed Consent in Online Surveys .................................. 8
   3.3 Respecting Participants’ Rights in Online Surveys ............................................. 9
   3.4 Consent Processes for Minors ............................................................................ 9
   3.5 Confidentiality Issues and Disclaimers .............................................................. 9
   3.6 Higher Risk Research ....................................................................................... 10
4. LEGAL AND COMPLIANCE ISSUES ..................................................................... 10
   4.1 Terms and Conditions of Social Media Platforms or Social Networking Apps .......... 10
   4.2 Copyright .......................................................................................................... 12
   4.3 Research Data Processing (including collection, storage and use) .................... 12
5. REFERENCES ........................................................................................................... 13
6. CHANGE HISTORY .................................................................................................. 13
7. APPENDIX A: COMBINED INFORMED CONSENT PROCESS FOR ONLINE SURVEYS ...... 15
1. **SCOPE OF THIS GUIDANCE**

Internet-mediated or Internet-based research (IBR) may be conducted in a variety of ways, including the use of microwork platforms such as Amazon Turk, and online survey tools such as Microsoft Forms (Nexus 365 version) and JISC Online Surveys, the running of experiments online, in-depth and large scale data mining of material already posted online (e.g., on blogs, discussion fora or social media sites such as Facebook and Twitter), or in-depth ethnographies of online communities. ‘Big data’ research and the technologies used to implement it may also come under the heading of internet-based research. Many instances of IBR can utilise and apply existing ethical codes that are used for more ‘traditional’ settings. However, there are some important differences. For example, informed consent is a key ethical issue in IBR, where participants and researchers do not usually meet face to face. In such cases it is harder to establish the age and competence of individuals to consent freely, and with understanding, to research participation. Researchers therefore need to consider how to meet their duty of care of participants in their research where there is no direct contact with them.

As this area is constantly changing due to advances in digital technologies it is essential for researchers to be very aware of the particular context they are working in and the expectations and assumptions of potential participants. In addition to this guidance, researchers are encouraged to look at the guidance for their ‘home’ discipline, as well as the detailed recommendations from the Association of Internet Research Ethics (AOIR, 2019), especially regarding general ethical guidelines and decision-making in IBR; and the Association of Computing Machinery’s (ACM) Code of Ethics and Professional Conduct.

Please note that Oxford staff and students will need to gain research ethics approval from CUREC before starting any research project involving human participants and/or personal data.

---

1 The University of Oxford’s Information Security team has approved the use of the online survey platforms Microsoft Forms (Nexus 365 version), JISC Online Surveys and Qualtrics for collection of all types of personal data, including confidential data. However, survey owners still need to consider data privacy requirements with respect to GDPR. All staff can access Microsoft Forms through their Nexus 365 account. IT Services manage an organisation-wide licence for JISC Online Surveys and any student, staff member or academic visitor can request an account for creating surveys – see IT Services’s JISC information webpage. In cases where Microsoft Forms, JISC or Qualtrics do not provide all the functionality required, RedCap is an alternative recommended by the University’s Information Security team. Researchers should take advice from Information Security about other third party providers who may collect or process personal data on their behalf, particularly if data is being processed outside of the EEA.


3 Association of Computing Machinery’s Code of Ethics and Professional Conduct (accessed 19 May 2020)

4 Please see the University’s Research Ethics webpages for information on how to apply for research ethics review at Oxford University. (accessed 19 May 2020)
2. **PUBLIC/PRIVATE ONLINE SPACE AND ETHICAL CONCERNS**

Research findings by Ipsos Mori (commissioned by the Carnegie Trust)\(^5\) stressed that public opinion is clearly divided when it comes to individuals’ publically available social media data being shared for research purposes - many would not expect their social media data to be used in this way\(^6\). Therefore more care must be taken in both consent and data management processes, to respect individuals and their privacy.

Even if social media posts or other online content are **publicly** available, a number of **ethical concerns** remain, e.g.:

- the post/data must not be misrepresented by the researcher;
- the user’s data must not be ‘triangulated’ in such a way that the researcher reveals identifying potentially harmful information that the user did not originally intend to share (e.g. linking Twitter posts with information on another platform by the same user).
- the potential to infer personal information from the information provided (e.g. gender from screen names or geographical location using analysis of text of photos) can be highly problematic. Full anonymisation of qualitative data may be very difficult.
- the post/data was published but has been subsequently deleted. (However, if such posts have subsequently been published elsewhere in publicly available media this is less of an issue.)
- the data is cited in such a way that makes the information easily findable (and thus traceable to the user) online
- even though individuals may use avatars or personas to create separate online identities or ‘alter egos’, **identification** and **recruitment** of these entities is subject to the same ethical considerations as the individuals themselves, where perhaps greater caution is warranted with respect to linkage between data arising from the persona and the true underlying identity. Note that UK and EU data protection law specify that e.g. usernames are considered personal data.

Please also refer to the very comprehensive list of internet-specific ethical questions which researchers should engage with ‘prior to, during, and after the research process’ that has been compiled by the Association of Internet Research Ethics (AOIR)\(^7\).

2.1 **Twitter**

Tweets are generally assumed to be public, however, the above ethical concerns apply. Please also see the decision matrices in the **Consent section** below.

\(^5\) See the Carnegie Trust’s report *Online Data Privacy from Attitudes to Action: an evidence review* (accessed 3 October 2019)

\(^6\) Jane Bainbridge (2015) ‘Call for better ethical standards in social media research’ and Academy of Social Sciences, *Summary* of Conference on ‘Ethical issues in social science research on social media’, March 2016. (both accessed 3 October 2019)

\(^7\) See the Association of Internet Researchers (AOIR), ‘Internet Research – Ethical Guidelines’. (Version 3.0, 2019) (accessed 09 December 2019)
2.2 Facebook and Similar Social Media Networking Services

Facebook posts and posts from similar networking services should only be assumed to be public if they have been set as publicly accessible (i.e. if researchers don’t have to ‘befriend’ participants/groups or ask permission to view them). Please note that e.g. “friends of friends” settings in Facebook are not counted as publicly accessible, as it would not be possible to gain informed consent from all “Friends of Friends” involved. It is the researcher’s responsibility to check the relevant social media platform’s terms and settings, and to think through their ethical implications. Again, the above ethical concerns also apply. Please also see the decision matrices in the Consent section below.

Please note that, generally, researchers should not ‘befriend’ their participants on Facebook, Twitter, or any other social media. See Zimmer (2010) for a valuable discussion of this\(^8\). In the case of research participants who are children this is especially important, but this also applies to adult participants. Please refer to the University Code on Safeguarding.

2.3 Message Boards/Chat Rooms

Individuals in chat rooms do not generally approve of being made research participants without their consent.\(^9\) and \(^10\) It is also important to note that message board or chat room posts should only be assumed to be public if they have been set as publicly accessible (i.e. if you don’t have to register or ask for permission to view them). Again, the above ethical concerns apply. Please also see the decision matrices in our Consent section below.

2.4 Mobile Internet Connections

Sensitive data from mobile internet connections (e.g., users’ location and contact details stored on smart phones and tablets, as well as the metadata of their communications) raise additional ethical issues – especially as there may be a possibility of re-identifying cases in ‘anonymised’ datasets. For a broad discussion of these issues and helpful practical and ethical guidelines for researchers using datasets constructed with information from mobile devices please see ‘Ethical Privacy Guidelines for Mobile Connectivity Measurements’ (2013)\(^11\).

2.5 Deception

‘Befriending’ participants under false pretences is not acceptable, though other forms of deception might be acceptable depending on the context of the research. Researchers who are planning to ‘befriend’ participants without revealing their identity or true intent will need to explicitly address the reasons why this is necessary in their ethics application. Please also see CUREC’s Approved Procedure on Deception.

---


\(^11\) Zevenbergen, Bendert and Brown, Ian and Wright, Joss and Erdos, David, Ethical Privacy Guidelines for Mobile Connectivity Measurements (November 7, 2013) (accessed 3 October 2019)
2.6 Dark Web Studies

If researchers need to access the Dark Web as part of their research study, it is recommended that they contact their IDREC or DREC in the first instance to discuss the planned research.

In addition, researchers will need to consult the following before accessing the Dark Web:

- the University IT regulations\(^\text{12}\), which stipulate (inter alia) that
  
  ‘7. Users are not permitted to use university IT or network facilities for any of the following:
  
  (1) any unlawful activity;
  
  (2) the creation, transmission, storage, downloading, or display of any offensive, obscene, indecent, or menacing images, data, or other material, or any data capable of being resolved into such images or material, except in the case of the use of the facilities for properly supervised research purposes when that use is lawful and when the user has obtained prior written authority for the particular activity from the head of his or her department or the chair of his or her faculty board (or, if the user is the head of a department or the chair of a faculty board, from the head of his or her division);
  
  (3) with the intention of drawing people into terrorism (contrary to the University’s statutory duty under Prevent); […]’

  (These regulations are a reminder not to engage in unlawful activity online. However, it should be noted that the University cannot protect its staff or students from police/security services action.)

- the researcher’s supervisor and Head of Department (as the key source of advice, as they will be aware of the research topic and research methodology),
- the University’s Information Security Policy, for advice on how to put in place appropriate security measures if accessing sensitive material (or material blocked on the University network)\(^\text{13}\)
- Emotional Impact/Vicarious Trauma information and guidance (particularly if accessing material could potentially cause distress to the researcher(s)\(^\text{14}\)
- CUREC ‘Prevent’ guidelines (only when relevant), if there is a risk that the research topic could potentially come within the scope of the ‘Prevent’ duty, which seeks to prevent people from being drawn into terrorism.\(^\text{15}\)

2.7 Deepfakes

Deepfakes (where Artificial Intelligence (AI) is used to manipulate multimedia content to present an event that did not actually occur) should be treated the same as other types of personal data, meaning that any analysis of them (beyond metadata) need to follow comparable rules (e.g. consent, paraphrasing, non-disclosure) to other visual/audio data used in IBR. Appropriate care should also be taken given that these videos may have been made with the intention to harm others/tarnish reputations.

\(^{12}\) Oxford University IT regulations, available from (accessed 3 October 2019)

\(^{13}\) University of Oxford’s Information Security guidance and policy, available (accessed 3 October 2019)

\(^{14}\) University of Oxford’s Emotional Impact / Vicarious Trauma information (accessed 20 May 2020)

\(^{15}\) See CUREC’s Best Practice Guidance on Prevent (accessed 20 May 2020)
3. **CONSENT ISSUES**

Current guidance differs in its recommendation for what constitutes valid consent in IBR. Common to the guidance, however, is the view that the type of consent obtained should be proportional to the risk of the research to participants. This will affect whether consent should be documented (using a separate form), whether that documentation should be in hard or soft copy (e.g. some guidance expressly forbids ‘electronic’ documented consent where documented consent is required), whether consent may be evidenced via other ‘implied’ means, or whether it may be waived altogether (in the case of data which is truly in the ‘public domain’).\(^{16}\)

### 3.1 Informed Consent in Social Media Research

As a general rule of thumb in social media research, if researchers need to ask permission or need a registration to view/gather data (e.g., via a moderator), then an informed consent procedure is likely to be needed.

A very simple flowchart may help with deciding whether specific consent is needed for collecting and/or displaying social media data in reports/publications:

<table>
<thead>
<tr>
<th>Publicly available data (i.e. no registration needed to view data)</th>
<th>General public</th>
<th>Public Figures(^{17})</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can researcher collect data without consent?</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Can researcher display data without consent?</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

versus:

<table>
<thead>
<tr>
<th>Not publicly available data (i.e. researcher needs to register or get moderator approval before viewing data)</th>
<th>General public</th>
<th>Public figures(^{18})</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can researcher collect data without consent?</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Can researcher display data without consent?</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Researchers who wish to display direct quotes and the username and picture of the person in their work (especially if it is published in any way) should normally seek informed consent to do this.


\(^{17}\) Decisions on what constitutes a public figure should be made on a case-by-case basis. Researchers may also find the following resource useful: C. Williams, *Researching Power, Elites and Leadership* (London: Sage, 2012) (accessed 31 October 2019).

\(^{18}\) See footnote 16.
especially in cases of very sensitive data (e.g., hate speech). They should contact the participants directly having decided which consent procedure should be followed (e.g., online information sheet, online consent form, click boxes).

If gaining informed consent is not possible, quotes should normally be paraphrased and usernames/pictures de-identified in order to protect the ‘participants’.

The following flowchart about reporting tweets and opt out consent process developed by Williams, Burnap and Sloan (2017)\(^\text{19}\) may be helpful (text version below)

---

Researchers may publish a tweet if one or more of the following applies:

- The tweet comes from a public figure account
- The tweet comes from an organisational account – either an organisational account that isn’t that of an individual organisation member, or the account of an individual organisation member who is not tweeting in a private capacity
- Opt-out consent has been deemed necessary, and consent has been given, or no reply has been received and the window for replying has expired
- Opt-in consent has been deemed necessary, and consent has been given

Researchers should seek opt-out consent to publish a tweet from a private account, or an organisation account where an individual organisation member is tweeting in a private capacity, as long as all of the following apply:

- The user is not identifiable as vulnerable
- The content of the tweet is not sensitive
- The tweet has not been deleted at the time of research/writing

Researchers should seek opt-in consent to publish a tweet from a private account, or an organisation account where an individual organisation member is tweeting in a private capacity, if one or more of the following applies:

- The user is identifiable as vulnerable
- The content of the tweet is sensitive
- The tweet has been deleted but the account has not been deleted
- The tweet and account have been deleted, but the researcher can find the ex-user’s contact details

Researchers should not publish if one or more of the following applies:

- Opt-in consent has been sought, and not received
- Opt-out consent has been sought, and consent has been refused
- The tweet and account have been deleted, and the researcher cannot find the ex-user’s contact details

3.2 Implied Consent and Informed Consent in Online Surveys

For certain types of low risk research, such as completion of a simple online questionnaire, completion and submission of the questionnaire implies that consent for the use of the questionnaire data has been given. However, the questionnaire should be preceded by written information about the project and its aims (including information about how the data will be stored and published and a tick box confirming that participants are 18 or over and agree to take part).

Researchers should also make clear whether data which a lay user may not be aware of, but which may provide researchers with more information than participants would intend to provide, (e.g. time stamps on tweets or posts, IP addresses) are intended for collection, or whether the cross-referencing of data sources is planned. Both the use of Meta data and cross-referencing carry a greater risk of privacy breaches for individuals and could affect their autonomy over their online information.

The points above may already be covered by online panels such as Google Consumer Surveys or YouGov which have their own quality control checking, but any independently created surveys should follow these guidelines.

Please use simple language. IBR is particularly susceptible to over-technical language and researchers recruiting lay participants should make every effort to explain participation in non-technical language.
3.3 Respecting Participants’ Rights in Online Surveys

Where participants interact with online research materials or researchers themselves to generate fresh research data, participants must be free to withdraw themselves and their data at any point in the research.

In order to do this, researchers should clearly signpost ways in which participants can withdraw at any point, e.g. by using a ‘withdraw’ or ‘exit here’ button which leads to a quick debrief page, confirming that data (including IP addresses) will not be retained. Alternatively, this information should be clearly stated in the Participant Information text with details on how to exit (e.g., by closing the browser window).

In order to give participants the right not to answer any questions they do not feel comfortable with, online survey questions should not be made compulsory. Although researchers could address this difficulty by, for example, providing the option ‘I prefer not to say’, one study found that providing this option actually primed participants to be more concerned about privacy issues. Accordingly, the appropriateness of ‘opt-outs’ will have to be judged on a case-by-case basis.

Further still, anonymity makes it very difficult for participants to withdraw retrospectively from the study after completing part or all of an online survey. The logistics of this process need to be understood by the researchers and research participants and the implications should be clearly stated in the Participant Information text before participants start the survey.

Depending on the risk level of the study, participants should ideally be provided with a comment box to ask questions or provide feedback about the survey, which could then be addressed on a separate FAQ webpage that will stay live until the end of the study.

Researchers should also ensure that online surveys are set not to collect IP addresses if possible. For example, when using some online survey platforms, by default, survey results will include the IP addresses of respondents. JISC Online Surveys does not automatically collect IP addresses.

3.4 Consent Processes for Minors

As with other types of research, it is expected that consent from a parent or legal guardian is required in IBR which recruits minors who are defined in this guidance as children under the age of 18, though exceptions may be made for youths classing as ‘Competent Youths’ (see related guidance on this topic in the Frequently Asked Questions (C12) section of the CUREC website as well as the Best Practice Guidance on Research with Competent Youths. Some guidance goes as far as to recommend offline processes for obtaining parental/guardian consent before conducting research with children or adults at risk.

3.5 Confidentiality Issues and Disclaimers

Privacy and confidentiality of data is more difficult to manage in IBR because researchers are not in control of online communication networks, leading to the risk of third-party interceptions.

---


Therefore, as in non-online studies, researchers should **avoid giving absolute promises of privacy or confidentiality in consent processes**, especially where the data to be collected are sensitive. Researchers should also be careful about how they publish information about rare (online) events, as data subjects will be easily re-identifiable. As part of information-giving prior to seeking consent, researchers should consider using disclaimers, e.g.:

- **General disclaimer**: ‘Although every reasonable effort has been taken, confidentiality during actual internet communication procedures cannot be guaranteed’.
- **For research using third party websites to administer surveys**: ‘Data may be stored on backups or server logs beyond the timeframe of this research project’.
- **For interviews conducted over email**: ‘Email is an unsafe form of communication for private responses. This is because email can be easily hacked. Therefore, you should only take part in the study if you/your company are prepared for your responses to be made public, even though the research write-up will not link any responses to individuals/companies.’

### 3.6 Higher Risk Research

It is important to assess the extent to which higher risk research should be conducted online. In some cases, it is not appropriate to do so, although it may seem so on first inspection. For example, some might argue that sensitive topics are best conducted online due to the benefits of the lack of need for face to face contact. However, there are clear issues that need to be considered – e.g. the differences between perceived and actual levels of anonymity and how further support can be provided to participants during and after the study.

Whether higher risk research should be carried out online needs to be made on a case by case basis. As part of this researchers may be expected to authenticate participants offline prior to commencing consent and data collection procedures online (see also consent processes for minors). This could include sending PINs generated for the purpose of a given research project to registered households via, for example, an electoral register. In such a scenario, research participants (here, authenticated by being a resident of a registered household) could then use PINs to enter online research environments.

### 4. LEGAL AND COMPLIANCE ISSUES

#### 4.1 Terms and Conditions of Social Media Platforms or Social Networking Apps

Generally, researchers should check, when planning their research, that they will not contravene the terms and conditions of the platforms or apps they are studying or using to conduct their research. If researchers do expect to breach any terms and conditions, this should be explicitly addressed in the research ethics application. Be aware that terms & conditions may be based on the laws of a country outside of the UK, and that these may change during the course of your research.

Applications will be judged on a case-by-case basis and should address the following:

i. whether there are different ways of conducting this research to avoid the breach of contract;
ii. whether similar types of research have been conducted previously;
iii. the degree of public interest in the research;
iv. the likely public benefit of the research;
v. the level of experience and supervision of the researcher(s);
vi. the degree of potential harm to participants in the research (including any possible re-identification of participants in the research);
vii. the degree of potential harm to the researcher(s) in conducting the research;
viii. the degree of potential risk associated with the processing of personal data associated with the research (and any possible breaches of data protection legislation);

ix. the potential reputational risk to the Department and the University from the breach of contract. Bear in mind that it may be necessary to seek advice from Legal Services and the Chair of CUREC (and potentially the Registrar) as appropriate, depending on the level of risk;

x. how the results of any such research should be published or publicised.
4.2 Copyright

Legal considerations of copyrighted material play into the public/private material debate, and thus into the ethical issues arising in IBR. Researchers should always check whether material they wish to use is protected by copyright law, as the fact that an image has been posted in a publicly accessible place does not mean that it has been placed ‘in the public domain’ and that it is not bound by copyright. Visual data posted on social network sites or other public sites can be owned and/or licensed in a particular way by the user who posted the data and/or by the individual(s) who originally created that visual data and/or by others. Consequently, there may be occasions when multiple permissions are needed in order to use internet-based data for research.

4.3 Research Data Processing (including collection, storage and use)

Please note that, according to University Policy, research data must be securely stored for a minimum of three years after publication (or public release of the research). Certain funders will ask for longer storage periods of, for example, 5 or 10 years.

The University must also comply with the Data Protection Act 2018 (DPA) and General Data Protection Regulation (GDPR), which requires, briefly and in part, that personal data:

1. be processed lawfully, fairly and in a transparent manner;
2. be collected only for specified, explicit and legitimate purposes, and not be further processed in any manner incompatible with those; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;\(^{22}\)
3. be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
4. be accurate and, where necessary, kept up-to-date;
5. not be kept as identifiable data for longer than necessary for the purposes concerned; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals\(^{23}\); and
6. be processed securely.

\(^{22}\) However, personal data processed solely for research purposes, archiving purposes in the public interest, or statistical purposes may be stored indefinitely, provided there are appropriate safeguards in place. (e.g. pseudonymisation, if appropriate). If researchers “justify indefinite retention on this basis, [they] must not later use the data for any other purpose – in particular for any decisions affecting particular individuals.” Researchers should not retain personal data ‘just in case’ this might become useful for the above purposes in future. See the ICO’s advice on limitations to data storage.

\(^{23}\) Ibid.
The above list is not exhaustive. For all key requirements, see the University's policy on data protection and research, a quick data protection checklist, and guidance on exemptions.

5. REFERENCES

All last accessed October 2019

- Association of Computing Machinery’s (ACM) Code of Ethics and Professional Conduct.
- Academy of Social Sciences Conference on ‘Ethical issues in social science research on social media’, March 2016.
- Carnegie Trust / Ipsos Mori (2018), Online Data Privacy from Attitudes to Action: an evidence review
- Central University Research Ethics Committee web pages, University of Oxford (including further discussion about informed consent)
- Gleibs, I. H. (2014), Turning Virtual Public Spaces into Laboratories: Thoughts on Conducting Online Field Studies Using Social Network Sites, Analyses of Social Issues and Public Policy.
- Internet-based research guidance document published by The Committee for the Protection of Human Subjects, University of California, Berkeley
- University of Oxford, Social Sciences Division’s advice on emotional impact / vicarious trauma information
- University of Oxford Information Security guidance and policy
- Wikipedia, EU-US Privacy Shield

6. CHANGE HISTORY
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| 6.0        | • Major changes to the sections about ‘Deepfakes’, ‘Higher Risk Research’ and ‘Legal and Compliance Issues’;  
• Clarifications on issues around public accessibility settings in social media platforms, and issues around analysing rare events that may endanger social media users’ anonymity;  
• Addition of new sections ‘Terms and conditions of social media platforms or social networking apps’ and ‘Copyright’;  
• Removal of the section about Safe Harbour/Privacy Shield (essential brief information having been moved to footnote 1);  
• Text from the previous ‘recruitment’ section split into more relevant sections;  
• Additional Guidance text on the preferred online survey suppliers JISC and RedCap;  
• Revisions to Appendix A – Template Information and Consent;  
• General text update.                                                                                                                                                                                                                                                                  | 5.3                  |
| 6.1        | • Updated to reflect the UK departure from the EU                                                                                                                                                                                                                                                                                                       | 6.0                  |
| 6.2        | • Guidance updated following Information Security’s approval of Qualtrics for online surveys;  
• Tweet flowchart added to the Informed Consent in Social Media Research section.                                                                                                                                                                                                                                                                   | 6.1                  |
| 6.3        | • Guidance updated following Information Security’s approval of Microsoft Forms for online surveys                                                                                                                                                                                                                                                  | 6.2                  |
7. **APPENDIX A: COMBINED INFORMED CONSENT PROCESS FOR ONLINE SURVEYS**

In the participant information — which is to be shared with participants before the online survey commences — written information is combined with a short online consent process achieved by a few simple tick-box questions used to establish age and consent itself. This way of obtaining consent is generally only appropriate when participants will *not meet face to face.*

*Please adapt this template for your own purposes, tailoring the information sheet to the participant group.*

Optional statements are highlighted turquoise – delete if not applicable to your research (then delete all advisory text – highlighted yellow).

---

**Name of Study**

**Ethics Approval Reference** xxxxxxxx

---

**General Information**

The aim of this study is to *give details as to the purpose/value of the study.*

We appreciate your interest in participating in this questionnaire/online survey. You have been invited to participate as you are *insert age range and inclusion/exclusion criteria*. Please read through this information before agreeing to participate by ticking the ‘yes’ box below.

You may ask any questions before deciding to take part by contacting the researcher (details below).

We *researcher name/department* at the University of Oxford in collaboration with *other institutions if applicable* are investigating *xx.*

Please give details of what will happen in the task/project, e.g.: You will be given some questions/scenarios to read and then asked to answer questions on *xx.* This should take about *xx* minutes. *No background knowledge is required.* [Add details about the purposes for which the information will be used, and by whom, including any third parties who may be given access to that information.]

**Do I have to take part?**

Please note that your participation is voluntary. If you do decide to take part, you may withdraw at any point during the questionnaire for any reason before submitting your answers by *pressing the ‘Exit’ button/closing the browser.* [If applicable] However, we are only able to reimburse participants who complete the full survey.

**How will my data be used?**
Your answers will be anonymous [if applicable], and we will take all reasonable measures to ensure that they remain confidential.

Your data will be stored in a password-protected file and may be used in academic publications. Your IP address [will/will not] be stored. [All questions are optional.] OR [We have included a ‘Prefer not to say’ option for each set of questions should you prefer not to answer a particular question.]

Research data will be stored for a minimum of three years after publication or public release.

[If applicable] The data that we collect from you may be transferred to, stored and/or processed at a destination outside the UK and the European Economic Area (“EEA”). By submitting your personal data, you agree to this transfer, storing or processing.

Who will have access to my data?

[If collecting personal data]: The University of Oxford [other institutions may also be relevant] is the data controller with respect to your personal data, and as such will determine how your personal data is used in the study. The University will process your personal data for the purpose of the research outlined above. Research is a task that we perform in the public interest. Further information about your rights with respect to your personal data is available from https://compliance.admin.ox.ac.uk/individual-rights.

[OR, if collecting anonymised data, including no IP addresses]: [Online Survey Provider Name] is the data controller with respect to your personal data and, as such, will determine how your personal data is used. Please see their privacy notice here [insert link]. [Online Survey Provider Name] will share only anonymised data with the University of Oxford, for the purposes of research.

Your information may be shared with [add names or general description of entities who may have access to the data and for what purpose, such as collaborators and sub-contractors for the project, including suppliers of tools and services for the project].

[If applicable:] We would also like your permission to use your anonymised data in future studies, and to share data with other researchers (e.g. in online databases). Any personal information that could identify you will be removed or changed before files are shared with other researchers or results are made public.

Responsible members of the University of Oxford and funders may be given access to data for monitoring and/or audit of the study to ensure we are complying with guidelines, or as otherwise required by law.

This survey/questionnaire/project is for an [Honours/DPhil/MPhil/etc.] project. The Principal Researcher is [researcher name], who is attached to the [relevant Oxford department] at the University of Oxford. This project is being completed under the supervision of [names of supervisors].

This project has been reviewed by, and received ethics clearance through, the University of Oxford Central University Research Ethics Committee [reference number].

Who do I contact if I have a concern about the study or I wish to complain?

If you have a concern about any aspect of this study, please speak to [insert researcher name and University email/tel.] or their supervisor [supervisor name and email/tel.], and we will do our best to answer your query. I/we will acknowledge your concern within 10 working days and give you an indication of how it will be dealt with. If you remain unhappy or wish to make a formal complaint, please contact the Chair of the Research Ethics Committee at the University of Oxford who will seek to resolve the matter as soon as possible [select relevant committee below]:
Chair, Medical Sciences Interdivisional Research Ethics Committee; Email: ethics@medsci.ox.ac.uk; Address: Research Services, University of Oxford, Wellington Square, Oxford OX1 2JD OR

Chair, Social Sciences & Humanities Interdivisional Research Ethics Committee; Email: ethics@socsci.ox.ac.uk; Address: Research Services, University of Oxford, Wellington Square, Oxford OX1 2JD OR

[only for applications reviewed by a Departmental Research Ethics Committee (DREC)] Chair, [insert relevant Departmental Research Ethics Committee name]; Email: [insert relevant departmental research ethics committee email address and postal address]

[For applications reviewed by the Oxford Tropical Research Ethics Committee (OxTREC), please insert the contact details for the local ethics committee which has reviewed your project].

Please note that you may only participate in this survey if you are 18 years of age or over.

☐ I certify that I am 18 years of age or over

If you have read the information above and agree to participate with the understanding that the data (including any personal data) you submit will be processed accordingly, please check the relevant box below to get started.

☐ Yes, I agree to take part