Central University Research Ethics Committee (CUREC)

Best Practice Guidance 06_Version 5.3

Title: Internet-Based Research (IBR)

Contents

1. Scope of this Guidance

Internet-mediated or internet-based research (IBR) may be conducted in a variety of ways, ranging from the use of platforms such as Qualtrics, Amazon Turk, SurveyMonkey or other online survey tools, to in-depth and large scale data mining of material already posted online, e.g. on blogs, discussion fora or social media sites (Facebook, Twitter, etc.). "Big data" research and the technologies used to implement it may also come under the heading of internet-based research. Informed consent is a key ethical issue in IBR, where participants and researchers do not usually meet face to face, and therefore it is harder to establish the age and competence of individuals to consent freely, and with understanding, to research participation.

This guidance will focus on research involving smaller numbers of participants (and related consent issues), since consent in big data or non-reactive IBR (e.g. analyses of "found text", data mining) is often

impractical, and the research must instead be ethically justified via public interest arguments. Please refer to the more detailed recommendations from the Association of Internet Research Ethics (AOIR, 2012) for broader guidance, especially regarding general ethical guidelines and decision-making in IBR[1].

Please note that Oxford staff and students will need to gain research ethics approval from CUREC **before** starting any research project involving human participants or personal data.[2]

This document will be updated as further resources and guidance become available.

2. Public/ Private Online Space and Ethical Concerns

Some consider that research conducted on materials posted on public online spaces (e.g. Twitter) uses data 'in the public domain', and therefore that obtaining consent is not necessary. Others argue that whether online space can be considered public or private is always in flux. Recent findings by Ipsos Mori [3] stressed that public opinion is clearly divided when it comes to their 'public' data being shared for research purposes - many would prefer their social media data not to be used in this way[4]. Therefore more care must be taken in both consent and data management processes, to respect individuals and their privacy.

Even if social media posts 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 potentially harmful information that the user did not originally intend to share;
- 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.)

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", compiled by the Association of Internet Research Ethics[5].

2.1. Twitter

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

---

[1] See "Ethical Decision-Making and Internet Research". Recommendations from the AoIR Ethics Working Committee (Version 2.0, 2012). Available at http://aoir.org/reports/ethics2.pdf, pp.4-8.

[2] Please see http://researchsupport.admin.ox.ac.uk/governance/ethics/apply for information on how to apply for research ethics review at Oxford University.

[3] Source: https://www.ipsos-mori.com/ourexpertise/digitalresearch/sociallistening/wisdomofthecrowd/commentandanalysis/responsibilityforthecrowd.aspx (accessed 1 April 2016)

[4] https://www.research-live.com/article/news/call-for-better-ethical-standards-in-social-media-research/id/4014180 and Academy of Social Sciences Conference on "Ethical issues in social science research on social media", March 2016. Summary available at https://www.acss.org.uk/news/dont-drink-tweet-ethical-issue-social-science-research-social-media/ (both accessed 1 April 2016)

[5] See "Ethical Decision-Making and Internet Research". Recommendations from the AoIR Ethics Working Committee (Version 2.0, 2012). Available at http://aoir.org/reports/ethics2.pdf, pp.8-12.

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). Again, the above ethical concerns apply. Please also see the decision matrices in our Consent section below.

Please note that, generally, researchers should not 'befriend' their participants on Facebook, Twitter, or any other social media. In the case of children or adults at risk as research participants this is especially important, please refer to the University Code on Safeguarding at www.admin.ox.ac.uk/personnel/cops/safeguarding/safeguide/.

2.3. Message boards / chat rooms

In a 2003 online study, individuals in chat rooms generally did not approve of being studied without their consent.[6] 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, such as users' location and contact details stored on smart phones and tablets, as well as the metadata of their communications, raise additional ethical issues – also because there may be a possibility of re-identifying 'anonymised' datasets. For a broad discussion of these and helpful practical and ethical guidelines for researchers using these datasets please see "Ethical Privacy Guidelines for Mobile Connectivity Measurements" (2013)[7].

2.5. Deception

Researchers 'befriending' participants without revealing their identity or true intent will need to address the reasons for this in their ethics application. Please also see our Approved Procedure on Deception at http://researchsupport.admin.ox.ac.uk/governance/ethics/resources/ap#collapse5-0.

2.6. Dark Web studies

If researchers need to access the Dark Web as part of their research study, they should contact their IDREC or DREC in the first instance to discuss whether formal ethical review is needed prior to their research starting.

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

---

[6] James. M. Hudson & Amy Bruckman (2004): Participant Objections to being Studied and the Ethics of Chatroom Research, The Information Society: An International Journal, 20:2, 135, http://www.tandfonline.com/doi/abs/10.1080/01972240490423030

[7] Zevenbergen, Bendert and Brown, Ian and Wright, Joss and Erdos, David, Ethical Privacy Guidelines for Mobile Connectivity Measurements (November 7, 2013). Available at SSRN: http://ssrn.com/abstract=2356824 or http://dx.doi.org/10.2139/ssrn.2356824 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2356824.

- the **University IT regulations**[8]**,** 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)[9]
- **Secondary Trauma** information and guidance (particularly if accessing material could potentially cause distress to the researcher(s)[10]
- **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.[11]

3. Recruitment

It is important to recognise that identification and recruitment of participants in IBR is challenging and has ethical implications. In high-risk research, researchers may be expected to authenticate subjects 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). Research subjects (authenticated by being the registered householder at an address) could then use PINs to enter online research environments.

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, with perhaps a greater caution about linkage between data arising from the persona and the true underlying identity.

[8] Oxford University IT regulations, available from www.admin.ox.ac.uk/statutes/regulations/196-052.shtml
[9] https://www.infosec.ox.ac.uk/guidance-policy
[10] https://www.socsci.ox.ac.uk/services/research-and-impact/fieldwork/files-1/secondary-trauma-for-researchers-and-supervisors-18-jan-16.docx (available from https://www.socsci.ox.ac.uk/services/research-and-impact/fieldwork/fieldwork)
[11] http://researchsupport.admin.ox.ac.uk/sites/default/files/researchsupport/documents/media/bpg_07_prevent_duty.pdf

4. 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"). [12]

4.1 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:

Publicly available data (i.e. no registration needed to view data)		
	Lay public	**Public Figures [13]**
Can researcher collect data without consent?	Yes	Yes
Can researcher display data without consent?	No	Yes

vs.

Not publicly available data (i.e. researcher needs to register or get moderator approval before viewing data)		
	Lay public	**Public figures[14]**
Can researcher collect data without consent?	No	Yes
Can researcher display data	No	No

[12] For a more detailed discussion of the public/private distinction, and some useful examples of social network site (SNS) research) 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. doi: 10.1111/asap.12036. Available at http://onlinelibrary.wiley.com/doi/10.1111/asap.12036/full.

[13] Decisions on what constitutes a public figure should be made on a case-by-case basis.
[14] See footnote 6.

without consent?

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, 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, etc.).

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

Generally**,** researchers should check that they do not contravene the terms and conditions of social media providers. If this is the case, this should be addressed in the research ethics application and will be judged on a case-by-case basis.

4.2 "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 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.

4.3 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 e.g. 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". [15] This will have to be judged on a case-by-case basis.

Anonymity makes it very difficult or impossible for participants to withdraw retrospectively from the study after completing part or all of an online survey. This should also 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 comments about the survey, which could then be addressed on a separate FAQ web page that will stay live until the end of the study.[16]

Researchers should also ensure that online surveys are set not to collect IP addresses if possible. E.g. in SurveyMonkey, by default, your survey results will include the IP addresses of respondents. You can turn on 'Anonymous Responses' to prevent IP tracking by going to the 'Collect Responses' section of your survey, clicking the name of the collector, selecting 'Show advanced options' and then clicking on "Anonymous Responses", selecting "On". Your changes are saved automatically.

4.4 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 (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 (http://researchsupport.admin.ox.ac.uk/governance/ethics/faqs-glossary/faqs#tab-1-2) as well as the Best Practice Guidance on Research with Competent Youths (http://researchsupport.admin.ox.ac.uk/governance/ethics/resources/bpg). Some guidance goes as far as to recommend offline processes for obtaining parental/guardian consent before conducting research with minor or mentally incompetent adults.

4.5 Confidentiality issues and disclaimers

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

Therefore researchers should **avoid giving absolute promises of privacy or confidentiality in consent processes**, especially where the data to be collected are sensitive. 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

[15] Allen, P. J., & Roberts, L. D. (2010). The ethics of outsourcing online survey research. *International Journal of Technoethics*, *1*, 35–48. doi:10.4018/jte.2010070104 and Kara Emery (2014) So You Want to Do an Online Study: Ethics Considerations and Lessons Learned, Ethics & Behavior, 24:4, 293-303, DOI: 10.1080/10508422.2013.860031

[16] Kara Emery (2014) So You Want to Do an Online Study: Ethics Considerations and Lessons Learned, Ethics & Behavior, 24:4, 301, DOI: 10.1080/10508422.2013.860031

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."

5. Legislative Aspects

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; thus there may be occasions when multiple permissions are needed in order to use internet-based data for research.

5.1 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 e.g. 5 or 10 years. Please see http://researchdata.ox.ac.uk/university-of-oxford-policy-on-the-management-of-research-data-and-records/ and http://researchdata.ox.ac.uk/home/managing-your-data-at-oxford/ethical-legal-commercial/ for further information.

At the same time, 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;[17]
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[18]; and
6. be processed securely.

The above list is not exhaustive. For all key requirements, see

[17] ICO GDPR guidance at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/ (accessed 25 April 2018). 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, such as pseudonymisation. 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 hold on to personal data 'just in case' this might become useful for the above purposes in future. See ICO's advice on this at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/ (accessed 18 June 2018).

[18] Ibid.

www.admin.ox.ac.uk/councilsec/compliance/dataprotection/. A data protection and research web page is available at https://researchsupport.admin.ox.ac.uk/policy/data, including a quick data protection checklist at https://researchsupport.admin.ox.ac.uk/policy/data/checklist.

5.2 Safe Harbor / Privacy Shield – what does this mean for your online research project?

Until October 2015, the so-called "Safe Harbor" principles enabled certain transfers of personal data from the European Economic Area (EEA) to the US to be compliant with European privacy laws; this affected processing of personal data undertaken by companies such as SurveyMonkey, Facebook, etc., which use US servers for even part of their processing. Under this scheme, US companies storing or otherwise processing data provided to them by persons or entities established in Europe could self-certify that they adhered to certain principles, in order to enable those European entities to comply with the obligations imposed on them via the EU Data Protection Directive.

In October 2015, the European Court of Justice declared that the Safe Harbor Decision was invalid. The European Commission and the United States agreed to establish a new framework for transatlantic data flows on 2 February 2016, known as the "EU-US Privacy Shield", which on 12 July 2016 was deemed "adequate to enable data transfers under EU law", although it had initially received serious criticism from European data protection regulators.

Generally, it would be preferable for Oxford University researchers not to use online tools that can't guarantee full compliance with European privacy laws. For example, Oxford University researchers may prefer to use Bristol Online Survey, which is fully compliant with all UK data protection laws.[19] However, it is noted that e.g. SurveyMonkey now adheres to Privacy Shield. Before using online tools for storing/transferring personal data or research data it is recommended to check whether these tools adhere to Privacy Shield (https://www.privacyshield.gov/list).

In practice it is acknowledged that the impact on research projects that rely on non-Privacy Shield-protected online tools may be minimal, especially if the research data does not involve special category (formerly "sensitive") personal data (as defined in the GDPR and DPA 2018) and will be collected and transferred with the informed consent of the research participant, who has been fully informed of the purpose of the research project and who knows that his/her data will not be used for purposes other than research.

Nevertheless, a data protection analysis should be undertaken on a case-by-case basis to ensure that researchers have taken all reasonable steps under the circumstances in order to ensure that they and/or the University is not in breach of its data protection obligations.[20]

The University of Oxford's Legal Services can advise on the implications of the new EU-US Privacy Shield Agreement, and may also advise on alternative mechanisms which can be put in place to allow for the

[19] Oxford University has an account with Bristol Online Surveys (BOS), which all members of the University can use free of charge. To request access to BOS please email help@it.ox.ac.uk.

[20] Many online tools process data outside of the EEA, so researchers should check those suppliers' terms, and wherever possible, aim to eliminate transfers outside of the EEA or seek advice on securing GDPR/Data Protection Act-compliant data processing terms.
Additionally, in certain situations, such as collaborations with other academic institutions, or where another sponsor exists, there may be multiple data controllers, with whom appropriate contractual data sharing terms should be in place. Researchers should list any other institutions that qualify as data controllers (being the entities who decide the purpose(s) for which the data is collected and processed) in their research ethics application and participant information sheet.

processing of personal data outside of the EEA compliant with UK legislation. IT Services are also currently looking into creating alternative, Oxford-based online survey and crowdsourcing tools.

6. References

- "Ethical Decision-Making and Internet Research". Recommendations from the AoIR Ethics Working Committee (Version 2.0, 2012). Available at http://aoir.org/reports/ethics2.pdf
- Academy of Social Sciences Conference on "Ethical issues in social science research on social media", March 2016. Summary available at https://www.acss.org.uk/news/dont-drink-tweet-ethical-issue-social-science-research-social-media/
- Allen, P. J., & Roberts, L. D. (2010): The ethics of outsourcing online survey research. *International Journal of Technoethics*, *1*, 35–48. doi:10.4018/jte.2010070104
- British Psychological Society Ethics Guidelines for internet-mediated research (available at http://www.bps.org.uk/system/files/Public%20files/inf206-guidelines-for-internet-mediated-research.pdf)
- Central University Research Ethics Committee web pages, University of Oxford (available at http://researchsupport.admin.ox.ac.uk/governance/ethics/. For further discussion about informed consent please see http://researchsupport.admin.ox.ac.uk/governance/ethics/resources/consent)
- Emery, Kara (2014): So You Want to Do an Online Study: Ethics Considerations and Lessons Learned, *Ethics & Behavior*, 24:4, 301, DOI: 10.1080/10508422.2013.860031
- 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. doi: 10.1111/asap.12036. Available at http://onlinelibrary.wiley.com/doi/10.1111/asap.12036/full.
- Hudson, James. M. & Bruckman, Amy (2004): Participant Objections to being Studied and the Ethics of Chat room Research, The Information Society: An International Journal, 20:2, 127-139, http://www.tandfonline.com/doi/abs/10.1080/01972240490423030
- Internet-based research guidance document published by The Committee for the Protection of Human Subjects, University of California, Berkeley (available at http://cphs.berkeley.edu/internet_research.pdf)
- LinkedIn, https://www.linkedin.com/pulse/euus-safe-harbor-torn-down-what-does-mean-market-research-kim-smouter
- *The Guardian*, www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection
- Wikipedia, https://en.wikipedia.org/wiki/International_Safe_Harbor_Privacy_Principles (accessed 1 April 2016)
- Zevenbergen, Bendert and Brown, Ian and Wright, Joss and Erdos, David (November 7, 2013): Ethical Privacy Guidelines for Mobile Connectivity Measurements. Available at SSRN: http://ssrn.com/abstract=2356824 or http://dx.doi.org/10.2139/ssrn.2356824 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2356824.

7. Appendix A: Combined Informed Consent Process for Online Surveys

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

Please adapt this template for your own purposes.

Name of Study

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 xx [add age range and inclusion/ exclusion criteria]. Please read through these terms before agreeing to participate by ticking the 'yes' box below. [If applicable] You may ask any questions before taking 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.

You will be given some questions / scenarios to read, and then answer questions on xx. It 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. 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 your data be used?

Your answers will be completely anonymous [if applicable], and we will use all reasonable endeavours to keep them 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 if 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, and stored or processed at, a destination outside the European Economic Area ("EEA"). By submitting your personal data, you agree to this transfer, storing or processing.

Who will have access to your 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.web.ox.ac.uk/individual-rights.

[Or, if collecting anonymised data, incl. 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 fully 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 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 questionnaire 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].

What if there is a problem?

If you have a concern about any aspect of this project, please speak to the researcher [researcher name and email/tel.] or their supervisor [supervisor name and email/tel.], who will do their best to answer your query. The researcher should acknowledge your concern within 10 working days and give you an indication of how they intend to deal with it. If you remain unhappy or wish to make a formal complaint, please contact the relevant Chair of the Research Ethics Committee at the University of Oxford [select relevant committee below]:

Chair, Medical Sciences Inter-Divisional 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 Inter-Divisional Research Ethics Committee; Email: ethics@socsci.ox.ac.uk; Address: Research Services, University of Oxford, Wellington Square, Oxford OX1 2JD **OR**

[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]

The Chair will seek to resolve the matter in a reasonably expeditious manner.

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