Checklist of General Data Protection Requirement (GDPR), 2016 and Data Protection Act (2018) points to take into account for research.

Please refer to the *Question Specific Advice for the Stage 1 Research Ethics Application* Form and *the Summary of the General Data Protection Requirement (GDPR) and Data Protection Act (2018*) for further information on the research ethics website.

For any further queries, please contact our Data Protection Officer at: dpa@aru.ac.uk

All researchers who will be collecting personal data need to complete the *Research Checklist for Data Protection,* available at:

https://myaru.sharepoint.com/sites/student-office-for/SitePages/data-protection-in-research.aspx#research-checklist-for-data-protection

Researchers do not need to submit this *Checklist* with their application, but need to confirm they will comply with the statements in Section 6 of the S*tage 1 Research Ethics Application Form.*

If researchers will be collecting special category data or intend to recruit 100 or more participants (Question 28 on the Stage 1 Research Ethics Application Form and 39 on the Stage 1 Research Ethics Application Form- Animals and Habitats), they will also need to complete the *Further Data Protection Questions* at:

https://myaru.sharepoint.com/sites/student-office-for/SitePages/data-protection-in-research.aspx#further-data-protection-questions

If they say 'yes' or 'not applicable' to all the questions, researchers need to submit this form with their ethics application. Should any of the responses be 'no' they must contact our Data Protection Officer for advice before they can submit to the FREP/SREP. Any changes requested by the Data Protection Officer must be made and all correspondence must be submitted with the ethics applications.

The UK GDPR and Data Protection Act (2018) applies to all research which involves 'personal data': ***Personal data*** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person**.**
The General Data Protection Requirement (GDPR) applies to the European Economic Area (EEA) countries, and UK GDPR is accepted as equivalent law there. The Data Protection Act (2018) also applies to the UK. Other countries in the EEA are likely to have their own data protection legislation which supplements GDPR and it is your responsibility as a researcher to check and comply with this.

Where research involves obtaining personal data from or sending personal data to organisations based outside the EEA (and the UK government trusted nations list) then additional agreement terms will need to be in place.
You must comply with data protection legislation of any other country you are carrying out research in.
Data does not fall under the legislation if anonymised, but context is key and you need to be confident that the data is truly anonymised (e.g. please see the Information Commissioner's *Code of Conduct, Anonymisation;* available at: https://ico.org.uk/media/1061/anonymisation-code.pdf and the *Motivated Intruder Test* at https://ico.org.uk/media/1061/anonymisation-code.pdf. If in doubt, you must treat the data as falling under the legislation or contact our Data Protection Officer for advice.
Anonymisation of data that you have collected itself counts as processing personal data.
If you need to collect personal data for the purposes of your research, you must only collect the minimum amount (this is known as *data minimisation*) and anonymise it as soon as possible.
If it is not possible to anonymise your data, you must pseudonymise it at the earliest opportunity (i.e. personal data for which identifiers are physically split and stored separately from the rest of the dataset, but kept within the same organisation).
Should you need to work with personal data, you should minimise its use as much as possible.
You should only share the data with those who need to know e.g. for students, your supervisor and this should be in anonymised or pseudonymised format, unless there is a rationale why this cannot be done.
You need to ensure that your research will follow procedures set out in the *Privacy Information for Research Participants.* which is available at: https://www.aru.ac.uk/privacy-and-cookies/research-participants
Research participants need to be informed about the legal basis for processing their data. The legal basis that can normally be relied on for research at our university is '*processing is necessary for the performance of a task carried out in the public interest'.* This information is in the *Privacy Information for Research Participants.*
Additional safeguards need to be in place if you will be processing 'special category data' and/or you intend to have 100 or more participants. This is because both of these create a greater data protection risk, which may require a statutory risk assessment to be completed.
Special category data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; and the processing of genetic data or biometric data for the purpose of uniquely identifying a person; data concerning health or data concerning sex life or sexual orientation. The law requires us to apply security over our data handling which is 'appropriate' to its sensitivity, therefore special category data will need additional protection.
You need to have an additional legal basis for processing special category data, which will usually be '*processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes'*.
You need to state on your own *Participant Information Sheet* whether ARU is the Data Controller, Joint Controller or Data Processor.
If you are using an Online Survey Platform, you should use *Online Surveys*, given it is based in the UK. Our Data Protection Officer has also approved *Qualtrics*. You cannot use any other online survey platforms without permission from ARU's Data Protection Officer.
If you will be collecting special category data, it is mandatory to use an EEA-based survey.
Once the closing date for the survey has passed, you must download the data onto University systems immediately and remove the data from the online survey.
Where there is a risk that the processing of personal data will cause substantial physical or psychological harm of financial loss to participants, it could be unlawful and must be considered carefully to see what can be done to reduce the risk of harm.

You must also ensure as far as possible that the processing will not be used to support measures or decisions with respect to a particular individual (the exemption to this is approved medical research).
If you plan on collecting data from existing records, you must ensure this complies with data protection legislation by having appropriate safeguards in place over the use of the data. You must obtain written permission from someone in the organisation who has the authority to provide this for collection of existing data. As part of good ethical practice, you must also cover this in the consent process with participants and include the fact you plan to do this on your *Participant Information Sheet* and as one of the statements on your *Participant Consent Form.* You must also consider what would happen if participants would like to take part in the research but do not wish existing data about them to be collected. Can they still participate or would they need to be excluded?

JS/CP

24 July 2019

Version 1.7

Updated: 26 October 2021

Version 1.8