2023

Data Transfer, Security and Confidentiality Agreement

This agreement is between the TIDES study and the recipient / receiving agency. It refers to the pseudonymised dataset provided by the TIDES study on an agreed date and for the purposes of data analysis as agreed by the TIDES steering committee.

I agree to abide by the following conditions:

- I understand that the TIDES study (1) retains all intellectual property rights in the data, (2) has sole publishing rights, and (3) has control over the content of any document that may result from these analyses.
- I will not pass on the data, data documentation, or results of the data analysis, or disclose any information relating to the data to a third party.
- I will not use the data or data documentation (e.g., topic guides, questionnaires, protocol documents) for any purpose other than as agreed with the TIDES Steering Committee.
- I confirm that I will destroy my copy of the dataset on completion of the work agreed upon with the TIDES Steering Committee or immediately upon request. I will acknowledge that I have deleted my copy in writing.
- I will not attempt to identify any study participant from the data (either via data linkage or by other means) and will report results in such a manner that participants cannot be identified. Low *n* results (i.e. <10) will be suppressed.
- Publication of analysis/results by MSc/PhD students subsequent to their project must be reported to and agreed by the TIDES Steering Committee.
- I agree to ensure the security of the data and the data documentation, preventing unauthorised access to the data and data loss.
- I understand that the data or data documentation (e.g., topic guides, questionnaires, protocol documents) must only be stored on and accessed via a secure King's College London server (e.g., R or N drive and KCL SharePoint) or a OneDrive for Business staff/student account, or other secure site agreed by the TIDES Steering Committee.
- I agree to ensure that the data or data documentation (e.g., topic guides, questionnaires, protocol documents) will not be downloaded, copied or stored on any personal devices/hardware (e.g., phones/tablets/PC/laptop/external hard drive/USB) or any web-based storage (e.g., iCloud/Google cloud and Dropbox).
- The data should be password protected; to comply with KCL policy the password should be at least 12 characters long. IT recommend using 3 random words with a mix of characters and symbols, e.g. 1hatePickle! Passwords should not be written down (i.e. use a password manager).
- I understand that before I am allowed access to the data I must undertake the online MRC Research, GDPR and Confidentiality Quiz and upon successful completion provide the project administrator with my certificate.
- I will report any loss of data, including such data which is encrypted, to the TIDES team immediately should they occur.

Date	
Signature	