

Undergraduate psychology research data protection and storage protocol

For all undergraduate research projects involving any form of primary data collection, the following protocol outlines the key procedures that should be followed to ensure the confidentiality and appropriate protection of participant data. This protocol complements and is in addition to the University and BPS guidance documents, which all psychological research within the department must adhere to at all time.

No recruitment or data collection can commence until the study has been approved by the School Research Ethics Committee (SREC) with a record of this approval on the student/project file.

		Student/supervisor checklist
1	All final consent forms, study information sheets, and debrief forms must be approved by the dissertation supervisor prior to data collection starting.	
2	Once approval has been given, it is the student's responsibility to ensure that appropriate consent is obtained from all participants, and that these consent forms are stored securely for the duration of the research.	
3	Signed consent forms MUST be kept separate from hard copies of questionnaires and other data.	
3.1	- If it has been deemed necessary to link consent forms and questionnaires through an ID number, then extra precaution must be taken to ensure that completed questionnaires are not stored alongside consent forms with a linked ID number. In large-scale studies it is good practice to create an "Identification key" which can be stored in a secure location whereby researchers can link the ID numbers back to the participant name if needed. - Linking consent forms and data should only be necessary if the researcher needs to collect follow-up data requiring the linking of research data across multiple time points. <i>For example, if conducting a questionnaire study where participants get sent a follow-up questionnaire two weeks after the first questionnaire is completed, then it will be necessary to link the ID numbers to the consent form in order to track participant responses/send participants further questionnaires.</i> - If consent forms and data are linked through the ID number then participants can in principle request the withdrawal of their data at any point during or after completion of the study. Consent and/or debrief forms should stipulate a timeframe for such withdrawal requests, which should normally state up until the aggregate analysis of anonymised data.	

3.2	• In many cases for undergraduate research, it is often not necessary to link the consent forms to the Questionnaires or data collected through an ID number. If you do not need to put an ID number on a consent form then you should not do so. It is good practice here to use a random ID number allocation for each new participant that takes part the study. This ensures that any hard copy or electronic data collected is anonymous and cannot be linked back to any specific consent form or participants. • It is essential in this scenario to ensure that the study debrief form is given to participants before they leave the study location, and that this debrief form clearly indicates that should the participant wish to withdraw their data they must do so before leaving that location.	
-----	---	--

4	Upon completion of data collection for any study, students must immediately hand over all signed consent forms to their module leader/supervisor for secure storage and confirmation of informed consent being received. These forms should be contained in an A4 envelope clearly marked with the study name, name of researcher, and module details.	
4.1	For module-related assignments (including dissertations) these consent forms will be destroyed by the module leader/supervisor through shredding once the work has been marked, moderated and passed by the examination board. Under no circumstances must students destroy consent forms without explicit approval from the module leader/supervisor.	
4.2	For other research studies within the departments (e.g., undergraduate assistantships), the consent forms will be stored by the lead researcher in a locked filing cabinet for the relevant duration of time in accordance with the data protection act.	

RESEARCH DATA: Any data collected through primary research involving human participants must adhere to the following good practice guidelines in addition to the Data Protection Act.

5.	All data collected must be stored securely and confidentially. Students and supervisors will need to agree on the most appropriate process for a specific research project, but the following guidelines must be adhered to as appropriate for a specific research design.	
5.1	Students must consider carefully the necessity of any personal data collected for a research project. <i>For example, if it is not necessary to analyse specific demographic data then do not collect it for the sake of it.</i>	
5.2	Hard copy questionnaires: Data from hard copy questionnaires must be inputted into the appropriate statistical package e.g., SPSS within 24 hours of data being collected from a participant. Hard copies must be stored with care and separately from consent forms at all times. As soon as all data has been inputted into an electronic spreadsheet, hard copies of the questionnaires must be handed in to the module leader/supervisor for secure storage/destruction of data as per 4.1 and 4.2 above (as appropriate).	

5.3	No identifiable data should be inputted into spreadsheets, with a unique ID number being allocated to each participant (in line with 3.1/3.2 above as appropriate).	
5.4	Where certain projects require the electronic storage of any personally identifiable data then file passwords must be put into place.	
5.5	For qualitative studies involving the recording of participants words through a digital recording device, the following steps MUST be followed: • Recordings must be downloaded onto a password protected file on the student's university network within 24 hours of each recording. • Once this has been completed and checked for correct downloading, the file MUST be deleted from the recording device. • Students must NOT store digital recordings on their home pc – only anonymised transcripts can be stored on home pcs or laptops. • Care must be taken to consider the contextual information provided by participants for qualitative studies. It may not be sufficient to simply remove the participants name and replace with a pseudonym or ID number. Contextual information may also need to be anonymised where necessary.	

Student declaration:

I can confirm that I have read the above protocol and have discussed the appropriate data protection and storage procedures for my study with my supervisor. (A copy of this signed form must be retained by both student and supervisor prior to data collection commencing).

Student Name: _____

Student Signature: _____

Date: _____

Supervisor Name: _____

Supervisor Signature: _____

Date: _____