**DPA Plan**

|  |  |  |
| --- | --- | --- |
| Ethics reference number: **41205** | Version: 1 | Date: 2018/04/25 |
| Study Title: POPS - App to Match People For Hobbies |
| Investigator: Ellena Parsons |

The following is an exhaustive and complete list of all the data that will be collected (through questionnaires, interviews, extraction from records, etc) The data that will be collected will include an anonymised ID for consent to take part in the survey, and the survey question responses.

The data is relevant to the study purposes because it will help us to better understand what a user wants from our application, thus assisting in our market research in designing and optimising our app. By attributing anonymised ID numbers, we are able to allow users to consent to taking part without having to collect personal identifying criteria.

The data will be processed fairly because participants agree to take part via consenting, and we will make users aware of what our survey is for and how it will be used.

The data’s accuracy is ensured because there will be multiple choice questions, and other questions which the user answers themselves. These will be transcribed word for word and unaltered.

Data will be stored on the laptops of our team, and once processed into our project will be subsequently deleted securely.

Data files will be protected by password and biometric login.

The data will be destroyed after being incorporated into the project. Modules finish by June 2018, and so deletion will be no later than this date.

The data will be processed in accordance with the rights of the participants because they will have the right to access, correct, and/or withdraw their data at any time and for any reason. Participants will be able to exercise their rights by contacting the investigator (e-mail: e.parsons@soton.ac.uk or the project supervisor DEM@soton.ac.uk).

Data is anonymised by assigning a randomised ID to each participant.

## Data Protection Act 1998 (DPA) best practice

If the study involves personal or sensitive data, explicitly explain how data will be collected, stored, analysed, held securely, and in turn destroyed. The DPA does not apply to anonymous data and a DPA Plan is not required in the case of such data.

The principles of the DPA are that personal data must be:

1. Processed fairly and lawfully.
2. Processed for specified purposes and in an appropriate way.
3. Adequate, relevant and not excessive for the purposes.
4. Accurate and up-to-date.
5. Not kept for longer than necessary.
6. Processed in accordance with the rights of data subjects (participants).
7. Protected by appropriate security, both practical and organisational.
8. Not transferred outside the European Economic Area (EEA) without adequate data protection controls.

Data is recorded information, whether stored electronically on computer or in paper-based filing systems. Personal data is information about an identifiable living individual. It can be factual, such as the date of a person’s interview, or an opinion, such someone’s view on how the person has performed on a task. It obviously includes individuals’ contact addresses or telephone numbers. (Less obviously, note that personal data is being processed where information is collected and analysed with the intention of distinguishing one individual from another and to take a particular action in respect of an individual. This can take place even if no obvious identifiers, such as names or addresses, are held.) Processing is any activity that involves data, including collecting, recording or retrieving, using, disclosing, organising, adapting, changing, updating, or destroying it.

The DPA identifies Sensitive Personal Data as:

1. the racial or ethnic origin of the data subject (participant);
2. his political opinions;
3. his religious beliefs or other beliefs of a similar nature;
4. whether he is a member of a trade union;
5. his physical or mental health or condition;
6. his sexual life;
7. the commission or alleged commission by him of any offence or
8. any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings and the sentence of court in such proceedings.

The processing of sensitive data must meet at least one of the 10 stricter conditions laid down in Schedule 3 of the DPA. It may be useful to know that condition 1 of this schedule permits processing of such data if the data subject has given his explicit consent, and condition 5 if the information has been made public as a result of steps deliberately taken by the data subject.

Keep in mind that the Police have a right of access to personal data held by the study for the purpose of safeguarding national security; preventing or detecting crime; prosecuting or apprehending offenders; assessing or collecting tax; or protecting the vital interests of the data subject or another.

Researchers are exempted: from the second data protection principle, meaning that personal data can be processed for purposes other than for which they were originally obtained; from the fifth data protection principle, meaning that personal data can be held indefinitely; and from the data subject’s right of access to his personal data provided the data is processed for research purposes and the results do not identify data subjects. In addition, the Data Protection (Processing of Sensitive Personal Data) Order 2000 para.9 provides that processing in the course of maintaining archives for research purposes is permissible where the sensitive personal data are not used to take decisions about any person without their consent and no substantial damage or distress is caused to any person by the keeping of those data. These exemptions do NOT give a blanket exemption from all the Data Protection Principles to data provided and/or used for research purposes. Researchers wishing to use personal data should be aware that the Data Protection Principles still generally apply, notably the requirement to keep data secure[[1]](#footnote-1).

A study may seek to anonymise the data it keeps. Anonymisation involves the removal of participants' personal information (names; e-mail address; whatever data it is that might permit identification; etc) from the data such that what remains cannot be used to identify them. Note that audio and video recordings (and often transcriptions too) cannot easily be anonymised, so they should normally be treated as non-anonymous data. Anonymised data can usually be kept without security and can easily be passed to other investigators for specialist analysis.

The DPA requires access to be granted to participants to all of their data, if any part of that data allows their identification. If the data has been anonymised, two issues arise.

1. If the personal information has been removed from the data AND DESTROYED, then the DPA is no longer applicable, and the data can be kept without security. However, investigators should note that they will be unable to follow up or subsequently contact participants in any way, or associate individuals with particular data, and should not attempt to suggest they might do so.

2. If the personal information has been removed from the bulk of the data, but NOT destroyed (ie, is kept separately), then the DPA remains applicable. In this situation, the personal information needs to be (a) kept both separately and securely from the anonymised data, and (b) to be linked or 'keyed' to the anonymised data, such keys to be similarly kept securely (and often kept with the personal information).

If personal data is collected, in the ‘Participant Information’, inform the participant of:

• the processes the study will take to ensure data security;

• their right to access and correct their data and their right to request removal of their data;

• the authority which will give them access to their data (provide the contact information).

If sensitive data is collected, or the study involves clinical studies, human tissue samples, invasive procedures, or young or vulnerable people, provide additional detail. In the ‘Participant Information’, inform the participant of:

• the separation of identifying data and the anonymisation process;

• the method of linking the consent form (if any) to the participant’s data;

• the processes for the destruction of all study data (if appropriate).

The study should conform to the University policy on data management applicable:

http://www.southampton.ac.uk/library/research/researchdata/

Investigators may find the University’s survey platform useful:

https://www.isurvey.soton.ac.uk/

# Contacts

 Research Support team, ergopse@soton.ac.uk.

1. http://www.jisc.ac.uk/publications/generalpublications/2001/pub\_dpacop\_0101.aspx [↑](#footnote-ref-1)