Faculty of Information - Ethics Application Common Mistakes

Ethics applications are often returned to researchers due to lack of information. Make sure you answer each question on the application, and provide clear and detailed information for the reviewer. REB reviewers often request more information Section 5 – Project Details and Section 11– Confidentiality and Privacy. Below is some advice on what to include in these sections.

Rationale & Purpose

- The reviewer needs to understand the overall study in order to properly assess the risks and benefits to human participants. Make sure to explain the full scope and rationale of your research, not only the part that involves human participants.
- Articulate your project with reference to academic or scholarly sources. Include full references at the end of this section.
- Write the rationale in plain language wherever possible. Avoid jargon.

Confidentiality

If you are guaranteeing confidentiality to your participants, then you must describe the ways in which you are protecting any information that could be used to identify the participants. Carefully read and follow the advice offered in the university’s Data Security Standards for Personally Identifiable and Other Confidential Data in Research. It is strongly recommended that students also familiarize themselves with Data Protection Measures.

Difference between Anonymous data vs. Anonymized data:

“Anonymous data” means that no identifiers will be collected during the study, while “Anonymized data” (also known as “de-identified data”) means that identifiers are collected but subsequently destroyed, such as a master list linking participants’ real name to their pseudonym.

Data Protection

The reviewer wants to know your plan for securing and storing the information you collect from participants for the full life cycle of the research (collection, use, dissemination, retention or disposal). Provide as much detail as possible. We have provided some common language that can be used where applicable.

Storage:

Paper information and data should be stored in a safe location that is “double locked”, such as in a lockable filing cabinet in a lockable office on campus.

Any electronic files that are not stored on a secure server must be encrypted. A password-protected folder or computer does not provide the same level of security as encryption. Learn the difference between Passwords vs. Encryption in this 20
An explanation of Microsoft Office file encryption is explained at 18:00, and additional security measures explained at 18:30.

Example text:

“All electronic files will be encrypted and stored on the researchers’ password-protected laptop”

“All electronic files will be stored on a secure server owned by and located in the Faculty of Information.”

“Paper data (e.g. fieldnotes, interview notes) will be stored in a locked cabinet located in a locked office in the Faculty of Information”

**Retention or Disposal:**

Provide a timeframe for how long you’ll keep the records for after the completion of the study. Time periods longer than a couple of years should be properly justified. Paper information and data should be destroyed using a shredder. Electronic information should be securely erased from the external hard drive, computer, or server that it is stored on.

Example text:

“All information and data will be disposed of two years after the completion of the study.”

“All information and data will be retained for five years after the completion of the study to allow sufficient time for the publication and other dissemination of research findings.”

“Paper records will be shredded. Electronic files will be securely erased from the researcher’s computer/secure server,”