Research Ethics

[UG Final Year Projects – CS Dept]

Session 2

Friday 21st October 2016

Frantzeska Kolyda – kolydaf@westminster.ac.uk
Research Ethics Departmental Representative


Ethics2

UG Project Students

All UG students undertaking their final project must consider the ethical aspects of their work in line with University procedures.

Please read carefully through the University's Ethics Code of Practice https://www.westminster.ac.uk/file/68476/download

To summarise: there are 2 Forms

Part A: Students should begin the process of consideration of research ethics approval by completing an Application Cover Sheet and the Part A application form.

If there are minimal ethical implications – see the decision tool at the end of Part A - then they will not need to complete the Part B application form.

Part B: If the research raises ethical issues, the student will be asked to complete Part B of the application.

Forms and Resources

The Coversheet, PART A and B forms (as well as PIS exemplar and Consent Form exemplar and further documentation) are found on Blackboard.

Also, your supervisor will be able to access the relevant intranet pages:

http://www.westminster.ac.uk/research/research-framework/research-ethics
(see towards the bottom of the page, links under ***Useful resources and tool-kit for applicants***)

https://myintranet.westminster.ac.uk/about-us/committees/current/research-ethics-committee/electronic-documentation-for-research-ethics-applications-for-all-undergraduate-students-except-psychology-students

Ensuring anonymity (examples)

The respondents are not required to give their identification like name or address.

Further ways of achieving anonymity could be a) the use of aliases or b) the use of codes for identifying people (to keep the information on individuals separate from access to them).

It is important to include in the questionnaire assurances of confidentiality, anonymity and non-traceability. This, for example, could be done by indicating that respondents do not need to give their name, that the data will be aggregated, that individuals will not be able to be identified through the use of categories or details of their location etc.

Consent (children and others) 1/2

Please read section 5.3 Informed Consent and the Participant Information Sheet
(University's Ethics Code of Practice https://www.westminster.ac.uk/file/68476/download)

Some participants may lack the ability to give their informed consent to participate in research, for example:

- **Children:** If school children are asked to be participants in a school-based environment, the Head Teacher of the school must be informed of what is proposed and give (in writing) their permission for pupils to take part. The parent(s) or guardian(s) consent should also be sought. Such permission is in addition to, not instead of, individual consent previously described. Minors must be informed that they have the same rights as an adult.

Consent (children and others) 2/2

- Those who lack competence for other reasons: In situations where participants are unable to give consent due to legal reasons, or are not able to understand fully the nature and consequences of what is proposed, written permission to participate must be obtained from the parent, guardian, person in authority, or person with legal responsibility for the participant. Such participants should be allowed to participate only on grounds of minimal hazard, absence of alternatives and sufficient potential social or medical benefit. Psychological illness or brain damage may or may not be sufficient to render the participant incompetent to give consent.

If you plan to use an online survey tool

Use **Google** survey tools (e.g. Google Forms) as the University controls a Google domain, under a compliant education sector (JISC Agreed) contract, so for non-sensitive personal data, this may suffice for your UG project.

For any sensitive data (e.g. medical, sexual life, religious or political views, etc.) online tools should probably not be an option for a UG project.

Data Security and Confidentiality

Relevant Data Protection legislation and University guidance in data security must be observed in the collection, use, storage, back-up and eventual destruction of all data.

Please read section 7. Research Data Protection and Security
(University's Ethics Code of Practice https://www.westminster.ac.uk/file/68476/download)

Guidelines on security arrangements for any recorded information (1/3)

1. Any recorded information should be adhered to the Data Protection Act 1998 requires that the participant's informed consent be sought where personal information is to be used and that those who have access to the information, or receive copies of it, are clearly identified.

2. Systems used for the storage of data should ideally be located on University Information Services' secure network infrastructure within the firewall so that access control measures and auditing policies can been forced.

3. Desktop/laptops used by researchers should always be fully patched and ideally, regularly scanned for software vulnerabilities.

Guidelines on security arrangements for any recorded information (2/3)

4. All the data held on recordable media (e.g. discs, USB storage devices) should be password protected as a minimum security measure, to protect the contents if they are lost.

5. Any recordable media containing identifiable personal data should be stored securely when not in use.

6. Knowledge of procedures and passwords to access any medical or research data of named individuals should be held securely and be made available only to those authorised.

Guidelines on security arrangements for any recorded information (3/3)

7. File protection (Encryption) should be in operation on computer systems used to hold named individual data.

8. Transmission of identifiable personal data across public communication lines (e.g. Email, DropBox etc.) should be avoided at all times. Where this is absolutely necessary, the prior approval of a Research Ethics Committee is required.

9. Access to the data should be directly supervised by a designated system manager and permitted only to those authorised by the Dean of Faculty.

Data Secure Disposal/Destruction

Once the project is complete and following the examination (and results), consideration must be given to the secure disposal and destruction of any data that is either, provided at the outset or gathered during the project.

Where personal information is involved, then specific measures to ensure the data is securely ‘deleted’ must be implemented.

Risk Assessment

Risk Assessment Form: (available on Blackboard) and also here (link accessible by your supervisor): https://myintranet.westminster.ac.uk/about-us/committees/current/research-ethics-committee/?a=187490:workspace%3A%2F%2FSpacesStore%2Fa6ed1fb6%2D024d%2D41f2%2D9020%2D0e94d74be072

It needs to be used if it is intended to collect data in specific circumstances e.g. in a venue outside the University, or even doing street interviewing, or if there is lone interviewing in a participant's home, but not for example if data is being collected from friends.

Please discuss with your supervisor the possibility that a Risk Assessment Form needs to be completed for your project.

Security Sensitive Situations

The Cover Sheet asks about security sensitive situations. At the moment there is no form for this, but if for example particular sites on the internet are going to be accessed, then that needs to trigger a Part B to be completed, and should go to FREC (Faculty Research Ethics Committee).

The Cover Sheet gives a link to look at but that link is now out of date – The University is looking into this but in the meantime the URL below is the up to date link:

http://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2012/oversight-of-security-sensitive-research-material.pdf#search=security%20sensitive

Good Luck!

Frantzeska Kolyda
kolydaf@westminster.ac.uk