Research, Business and Innovation

Policy on Conducting Sensitive Research

DATE 2016

1 Introduction and purpose

1.1 The university endorses the principle of academic freedom in relation to all research conducted under its auspices. However, all research must receive proper ethical approval, and researchers must follow appropriate processes for conducting the research and storing the related research materials. This is particularly important in relation to sensitive research.

1.2 In operating this policy, the university seeks to ensure that the freedom to pursue academic research is upheld, balanced with the need to protect both staff and students, and to ensure compliance with relevant legislation. See the Freedom of Expression and Academic Freedom (FoE) policy for more information.

1.3 The university aims to support the research activities of staff and students. Research into certain sensitive areas has a degree of personal risk for the researcher(s) undertaking it. Adherence to this policy will allow the university to assist external authorities by demonstrating that the actions of the researcher(s) were part of legitimate research activities. However, the university cannot guarantee protection from investigation by external authorities.

1.4 The university reserves the right not to grant ethical approval for any research which does not identify and address risks appropriately within the ethical approval application.

2 Scope

2.1 The policy's obligations shall apply to:

i. the university (which shall include all bodies or persons having authority to determine any matter relevant to this policy);
ii. anyone doing research under the auspices of the university (including all duly enrolled taught students, postgraduate taught students, or postgraduate research students of the university, whether full or part-time);
iii. all research projects, whether funded or unfunded, conducted on behalf of the university.

2.2 The policy's rights shall apply to anyone conducting research under the auspices of the university.

2.3 This policy should be understood in relation to the provisions of the Email, Internet and Social Media Policy.

2.4 Students are reminded of the relevant clauses in the General Student Regulations (Chapter 2, Student Discipline), and the Code of Practice for Research Degree Students, and Research Degree Regulations (2015).

3 Duties and responsibilities

3.1 It shall be the duty of all those subject to the policy to assist the university in adhering to the process for undertaking research in terms of proper ethical approval, storage of data and research materials, and dissemination (if any) of research materials.

3.2 Those under a duty to observe and uphold the principles of ethical research and academic freedom (see 4) within the university shall do so at all times while working for or on behalf of the university.

3.3 Senior researchers, including, but not limited to: Principal Investigators, Doctoral and Dissertation Supervisors, and

7.3 The offer letter will confirm the classification of sensitive research and the Conditions of Acceptance and Enrolment document will specify the special conditions required as part of the research. Ethical approval, as with all research degree students, must be applied for by the student within 6 months of enrolment. Failure to do so will mean the student will be strongly advised to cease working on any aspect of the research classified as sensitive.

7.4 A decision on whether ethical approval will be given to the student, including any changes that may be required, will be made by Faculty Ethics Committees within three months of the submission of the application for ethical approval.

8 Supervisors

8.1 Any PhD research project that meets the criteria of sensitive research will need to be acknowledged as such through the faculty confirmation on the Faculty Decision Form as part of the admissions process.

8.2 For all PhD projects involving sensitive research, both supervisors (first and second) will need to be actively involved in reading the student's work and supporting them in identifying potential risks and mitigating against them (including the potential for harm to the mental health and wellbeing of students) fn

11.3 Access to this Secure File Share must

14.1 Breach of this policy through failure to gain ethical approval for sensitive research, deviation from the research design originally submitted for ethical approval, or failure to store research materials for research into the areas listed in 11.1 securely, forfeits any protection the university can offer should external authorities launch an investigation. Normally breaches of this policy by both staff and students will be investigated through the Misconduct in Research – Investigation Procedure.

15 Policy rev5(y)lly

Appendix 1: Questions for Ethical Approval of Sensitive Research

Section A: Sensitive Research

1.

Section B: Accessing Websites for the Research Areas Outlined in Category Q5a

1. Will your research involve visits to websites that might be associated with radicalisation or terrorist/extremist organisations or groups?

Yes ☐ No ☐

If you answer 'Yes' to Q1 you are advised that such sites may be subject to surveillance by the police and accessing those sites might lead to police enquiries. It is strongly recommended that you use your university network address, once you have received ethical approval, which will ensure these activities are flagged as a legitimate part of your research. Whilst acquiring ethical approval for this project and adhering to University guidance on accessing websites and storing related materials securely will allow the University to verify the legitimacy of you accessing these websites, it cannot guarantee legal protection.

Please acknowledge that you understand this risk by putting an 'X' in the 'I Agree' box.

I Agree ☐

Section C: Storage and Transmission of Research Materials

The secure storage of data and research material is strongly recommended to all who answered 'Yes' in Section A, Q5 (although all researchers may make use of the ITMS provisions detailed in this questionnaire). Please note that anyone storing participants' personal data is subject to separate legislation and requirements. Details are outlined here, and in the university's Research Records Retention Policy.

1. Does your research involve the downloading and storage on a computer of any materials relating to extremism or radicalisation (for example, records, statements or other documents)?

Yes ☐ No ☐

If you answered 'Yes' to Q1, you should request a secure file share from ITMS to be created for your project, with access restricted to you, or if absolutely necessary, any internal co-investigator(s). The research materials should not be kept on a personal computer, and all online research in this area should be done on university servers[vii]. Physical data should be scanned and uploaded to the password-protected server; where this is not possible, it should be kept in a locked filing cabinet or similar on university premises.

You will need to agree to store all materials relevant to Section B, Q1 and Section C, Q2, as well as any other materials related to your research project in accordance with this advice in order to gain ethical approval.

Please confirm you will store all research documents in accordance with t his advice by putting an 'X' in the 'I Agree' box.

I Agree ☐

2. Might your research involve the electronic transmission of such materials to project Co-Investigators?

Yes ☐ No ☐

Note: The Terrorism Act (2006) and the Counter-Terrorism and Security Act (2015) outlaw the dissemination of terrorist publications if the individual concerned has the intention to encourage or induce others. Publications disseminated for the purposes of an approved and clearly defined research project should not amount to an offence, because the requisite intention is unlikely to be present. However, you are advised to exercise caution and avoid dissemination of raw research materials where possible.

You will need to agree to only transmit these materials to Co-Investigators after they have been password-protected and that you will only use 'Zend[viii]', which encrypts materials in transmission.

Please confirm you under stand the risks in disseminating publications and that you will only transmit these materials to collaborators after they have been password- protected and via 'Zend'.

I Agree ☐

---

[i] Illegal activities incorporates any illegal activity; for example, trespassing, theft, or online piracy.
[ii] Hate Crimes are those committed against someone because of their disability, gender-identity, race, religion or belief, or sexual orientation.
[iii] Harmful and illegal cultural practices : these include violence against women and girls, Female Genital Mutilation (FGM), forced marriage, child sexual exploitation and honour-based violence.
[iv] Accessing prohibited websites: You will need to seek permission from ITMS; advice on how to gain permission is available from the ITMS helpdesk.
[v] Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism
[vi] De-radicalisation usually refers to activity aimed at a person who supports terrorism and in some cases has engaged in terrorist related activity, which is intended to effect cognitive and/or behavioural change leading to a new outlook on terrorism and/or disengagement from it.
[vii] Secure File Share: You will need to ask ITMS to create a Secure File Share for your project, with access restricted to yourself, or if absolutely necessary, any internal co-investigator(s). Advice is available from the ITMS helpdesk.
[viii] Zend: advice on using Zend is available from the ITMS helpdesk.