

Policy on Conducting Sensitive Research

Contents

1	Introduction and purpose.....	3
2	Scope.....	3
3	Duties and responsibilities	3
4	Academic Freedom	4
5	Sensitive Research	4
6	Undergraduate and Taught Postgraduate Students and Sensitive Research	4
7	Postgraduate Research Students and Sensitive Research	4
9	Approval	5
10	Accessing Prohibited Sites	6
11	Storing Material	6
12	Transmitting Material	7
13	Raising Concerns	7
14	Breach of the policy	7
15	Policy review.....	8

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 Heads of School/Department, have particular responsibility for ensuring that all research undertaken by university staff and students has received full ethical approval before the research is conducted.

4 Academic Freedom

- 4.1 The university endorses and adopts the principle of freedom of speech and expression within the law. (See the **Freedom of Expression and Academic Freedom** (FoE) policy).

5 Sensitive Research

- 5.1 There are three broad research areas which would usually cause the research to be classified as 'sensitive':
- i. Research into illegal activities, including the collection of source data, e.g. crime statistics;
 - ii. Research which requires access to web sites normally prohibited on university servers; including, but not limited to; pornography, or the sites of any of the [organisations](#) proscribed by the UK Government. See section 10 of this policy for more details;
 - iii. Research into extremism and radicalisation.
- 5.2 The definition of sensitive research encompasses a wide variety of research topics, and it is a requirement to complete the relevant questions in the Faculty Ethical Approval Application Forms, in order to ascertain if a research project is likely to be considered sensitive research in accordance with this policy (see Appendix 1).

6 Undergraduate and Taught Postgraduate Students and Sensitive Research

- 6.1 It is not normally appropriate for students at this level to undertake any sensitive research due to their relative inexperience with research, and research ethics and protocols. In addition, supervisors and tutors will need to give careful consideration to the potential for some sensitive research areas to cause harm to the mental health and wellbeing of students.

7 Postgraduate Research Students and Sensitive Research

- 7.1 The Faculty Decision Form, used as part of the admissions process and sent to the Graduate School Office by the member(s) of academic staff recruiting the student will contain a similar set of questions to those in Appendix 1. Where a PhD project is defined as sensitive research, this will generate a specific non-standard offer letter and Conditions of Acceptance and Enrolment Document for the student.
- 7.2 If the proposed PhD project concerns a sensitive research area, faculty staff involved in the recruitment of the student should consider whether the student can be appropriately supported in undertaking their research, throughout the course of the research degree programme. Any special provisions, facilities or resources such as IT access to normally prohibited sites or secure storage of materials, should be identified by the faculty. In issuing an offer to a student the faculty will be confirming that such special arrangements can be provided throughout the length of the research degree programme. This will need to be agreed within the faculty before an offer is made to the student.

- 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).
- 8.3 Supervisors should also be conscious of the potential issues in finding suitable internal assessors for a reviewer for registration, an independent assessor for the annual review, and an internal examiner for the viva (who must be a different person from the independent assessor for formal review). Additionally, there are potentially difficulties in finding a suitable external examiner for the oral examination (viva). Due to these possible problems, arrangements should be made as early as possible.

9 Approval

- 9.1 The Faculty Ethical Approval Application Forms contain a sensitive research appendix with a series of filter questions (Appendix 1). These identify if a research project should be classified as sensitive research, and as such require special consideration before ethical approval can be granted.
- 9.2 Faculty Ethics Committees will make a collective decision whether or not to grant sensitive research projects ethical approval. The Chair and at least one other member of the committee will discuss the application and decide whether to give ethical approval, or to request changes to the research design/protocol.
- 9.3 Faculty Ethics Committees are acting on behalf of the university in making decisions to give ethical approval. Decisions must be based on the principles of freedom of speech and academic freedom in accordance with the **Freedom of expression and academic freedom** (FoE) policy. All Faculty Ethics Committee meetings must be minuted.
- 9.4 A decision on whether ethical approval will be given to the applicant, 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.
- 9.5 Applicants who are refused ethical approval with no option to amend their research design/protocol (something which should be very rare) may approach the Chair of their Faculty Ethics Committee for further information and advice. If the applicant is still dissatisfied with the outcome, they may appeal in writing to the Chair of the University

Human Research Ethics Committee (UHREC) for further consideration by appropriate members of the committee.

- 9.6 Any deviation from the research design granted full ethical approval is not permitted. If the research requires any change, such as accessing new materials, or undertaking new areas of investigation, then a resubmission for ethical approval will need to be made. Every effort will be made by the Faculty Ethics Committees to process this new application as rapidly as possible so as not to delay the research.
- 9.7 Once a Faculty Ethics Committee has granted ethical approval to a research project classified as sensitive, the project details will be recorded on a register by the Servicing Officer to the Faculty Ethics Committee. The details will then be sent to the Servicing Officer for UHREC, who will share an up-to-date copy of the register with the Director of Library and Learning Services and the Head of Security, Estates and Commercial Services.
- 9.8 UHREC will oversee the implementation of this policy and the approval process.

10 Accessing Prohibited Sites

- 10.1 Researchers whose projects have received full ethical approval and who require access to web sites normally prohibited on university servers must contact ITMS to arrange for special provisions to be made.
- 10.2 Researchers who access web sites that might be associated with radicalisation or terrorist/extremist organisations or groups should be conscious that such sites may be subject to surveillance by the police, and that accessing those sites might lead to police enquiries. Once full ethical approval has been granted, researchers should use the university network to access such sites. This will ensure these activities are flagged as a legitimate part of their research. However, as stated in 1.3 of this policy, the university cannot guarantee protection from investigation by external authorities.

11 Storing Material

- 11.1 Certain types of sensitive research require additional considerations, including
- i. Research into terrorism, extremism, terrorist or extremist organisations or groups, extremist ideologies, radicalisation¹, de-radicalisation²;
 - ii. Research commissioned by the military or GCHQ;
 - iii. Research commissioned under an EU / US security call or similar;
 - iv. Research involving the viewing, usage or transfer of sensitive personal data as defined as such by the Data Protection Act 1998;
 - v. Research involving the acquisition of security clearances (including the Official Secrets Act).
- 11.2 All research materials and data for research into the areas listed in 11.1 must be stored securely in a password-protected central store. No copies should be kept in any other location. If provision for secure storage has not already been arranged as part of the project, it is the responsibility of the researcher to contact the ITMS Helpdesk to request a Secure File Share.

1 Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism.

2 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.

- 11.3 Access to this Secure File Share must be restricted to the researcher, and any internal co-investigators working on collaborative projects. The secure storage arrangements must include all materials related to the research project, including but not limited to: downloads, documents, videos, images, or research data. Access to this Secure File Share can be revoked if the researcher leaves the project, or fails to comply with this policy.
- 11.4 Online sensitive research that has received ethical approval into the areas listed in 11.1 should be conducted on university servers (see 10.2).
- 11.5 Physical documents and 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.

12 Transmitting Material

- 12.1 Researchers should note that 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 a clearly defined research project should not amount to an offence, because the requisite intention is unlikely to be present. However, caution is advised and the dissemination of raw research materials should be avoided where possible.
- 12.2 In the instance of collaborative research projects with researchers at other institutions in the UK or abroad, the sending of documents may occasionally be necessary. Documents should be individually password-protected where possible, and then sent using 'Zend', which encrypts the file during transmission. Co-Investigators from outside the university may also use 'Zend' to send files to researchers at DMU, which must then be stored immediately in the secure file share. The ITMS Helpdesk can provide advice on 'Zend'.
- 12.3 Researchers are strongly advised to avoid transporting raw research materials connected to sensitive research projects. However, if it is unavoidable researchers should use an encrypted memory stick available from Faculties and ITMS.
- 12.4 Researchers should exercise caution when using personal social media to disseminate critical arguments or the outputs or outcomes of sensitive research projects for the reasons stated in 12.1. In particular, it is strongly advised that researchers do not create hyperlinks to sites used, with ethical approval, as 'raw research materials' (e.g. sites of any [proscribed organisations](#)). Additionally, researchers should adhere to the **Email, Internet and Social Media Policy**.

13 Raising Concerns

- 13.1 If anyone has genuine concerns related to the use or misuse of sensitive research materials by any member(s) of staff or student(s) they should contact the Head of Security, via telephone (0116 257 7642), or email (leicestersecurityoffice@dmu.ac.uk) in non-urgent situations. If the concerns relate to the content of any hard copy materials (e.g. books or printed papers) the materials should be left untouched, but the finder should stay with them whilst a senior member of the Security team verifies if these materials relate to a legitimate research project.

14 Breach of the policy

- 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 review

- 15.1 This policy will be reviewed periodically and amended if necessary.

In formulating this policy, the university has been informed by:

- Newcastle University – *Research Web Pages*
- University of Kent – *Ethics Review Checklist for Research with Human Participants*
- University of Exeter – *Terrorism Code of Conduct*
- Universities UK – *Oversight of security-sensitive research material in UK universities: guidance*

Appendix 1: Questions for Ethical Approval of Sensitive Research

Section A: Sensitive Research

1. Does the intended research include research into illegal activitiesⁱ? (This may include, but is not limited to, research into hate crimeⁱⁱ, theft, fraud, or harmful and illegal cultural practicesⁱⁱⁱ, the collection of source data, such as crime statistics, etc.).

Please note: the university does not permit any crime to be committed for research purposes, such as accessing images of paedophilia or child abuse, unless special permission has been granted by the Home Office.

Yes No

2. Does the research involve deception?

Yes No

3. Will the research require the use of sites usually prohibited on university computers (e.g. pornography or the sites of these [prohibited organisations](#))?^{iv}

Yes No

4. Has the research been commissioned under a commercial contract requiring secure storage for related materials?

Yes No

5. Does the intended research fit into any of the following categories? If so, please indicate which*:

- a.** Terrorism, extremism, terrorist or extremist organisations or groups, extremist ideologies, radicalisation^v, de-radicalisation^{vi}:

Yes No

- b.** Commissioned by the military or GCHQ:

Yes No

- c.** Commissioned under an EU / US security call or similar:

Yes No

- d.** The viewing, usage or transfer of sensitive personal data as defined as such by the Data Protection Act 1998?

Yes No

- e.** Involve the acquisition of security clearances (including the Official Secrets Act):

Yes No

***If you are unsure as to whether your research will involve any of these categories you are advised to answer 'Yes' to the most relevant.**

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 this 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 understand 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](#).