Policy on Researching and Handling
Sensitive, Extreme or Radical Material
# Contents

Introduction ............................................................................................................................................ 3  
Application of this Policy......................................................................................................................... 3  
Duties and Responsibilities ..................................................................................................................... 4  
Sensitive Research .................................................................................................................................. 4  
The Role of the Supervisor(s) .................................................................................................................. 5  
Approval Process..................................................................................................................................... 5  
Accessing Sensitive Websites.................................................................................................................. 6  
Storage, Transmission and Destruction of Electronic Material .............................................................. 7  
Further Guidance .................................................................................................................................... 8  
Training ................................................................................................................................................... 8  
Breach of the Policy ................................................................................................................................ 8  
Update and Review................................................................................................................................... 9
Policy on Researching and Handling Sensitive, Extreme or Radical Material

Introduction

1. The University carries out a wide range of research and the principles of academic freedom and freedom of speech underpin all research and teaching. However, all research must receive proper approval, and researchers must follow appropriate processes for conducting the research and storing the related research materials. This Policy is a sub-policy of the University’s ‘Research Code of Conduct’.

2. Universities play a vital role in carrying out research on issues where security-sensitive, radical or extreme material is relevant. It is not the intention of this policy to prevent or restrict sensitive research but accessing, storing and circulating security-sensitive, extreme or potentially radical research material is sometimes open to misinterpretation by the authorities, and can put authors in danger of arrest and prosecution under, for example, counter-terrorism legislation.

3. It is a duty of the University to ensure research into radical or extreme material, including chemicals or organisms that can be used as weapons, is carried out appropriately and with due regard to safeguarding the individual and others.

4. 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 or prosecution by external authorities.

5. 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 ‘Code of Practice Concerning Freedom of Speech’ and ‘Research Code of Conduct’ for further details.

6. The University reserves the right not to grant approval for any research which does not identify and appropriately address risks highlighted within this Policy.

7. This Policy does not replace the requirement for approval of projects with, for example, safety considerations such as use of genetically-modified organisms or dangerous chemical, but is intended to function alongside these other existing requirements.

Application of this Policy

8. This Policy applies to the following;
   - full time, part time or agency staff in any of the University’s job families (teaching and research, technical and experimental, management and administration, and community and operational), including Honorary Staff and Emeritus Professors;
   - staff visiting from other institutions undertaking or supervising research at or for the University; and

---

1 [http://www2.le.ac.uk/offices/researchsupport/full-code-of-conduct](http://www2.le.ac.uk/offices/researchsupport/full-code-of-conduct)
2 [http://www2.le.ac.uk/offices/sas2/regulations/documents/freedom_of_speech.pdf](http://www2.le.ac.uk/offices/sas2/regulations/documents/freedom_of_speech.pdf)
• undergraduate and postgraduate students (both taught and research), whether registered here or on temporary placement.

The term ‘researcher’ is used in this Policy as a general term to cover all of the above groups.

9. This Policy also covers those involved in fundraising, providing consultancy, innovation, commercial and analytical services and those involved in the setting up and running of University spin-out companies.

10. It should be noted that researchers based overseas or researchers travelling to overseas locations will need to abide by local laws and regulations in regard to collecting and holding sensitive data. It is the responsibility of the researcher to ensure that they familiarise themselves with these local rules prior to travelling or, if locally based, prior to starting research. It may be that University IT equipment is not available to manage such data, however this approval process should still be used to agree the protocols and effectively manage the risk. Note: This approval process may not protect individuals from action taken by other countries’ security or legal agencies

Duties and Responsibilities

11. It is the duty of all those subject to this Policy to assist the University in adhering to the process for undertaking research in terms of proper approval, storage of data and research materials, dissemination (if any) and secure destruction of research materials or outcomes.

12. Supervisors must ensure they understand their role and ensure suitable support is provided for those who carry out research and may be vulnerable to harming themselves or others through their actions; this is termed ‘safeguarding’.

13. Senior researchers, including, but not limited to: Principal Investigators, Doctoral and Dissertation Supervisors, and Heads of College/Department, have particular responsibility for ensuring that all research undertaken by anyone under the University’s auspices has received full approval in accordance with the ‘Research Code of Conduct’ and this Policy before the research is conducted.

Sensitive Research

14. There are four broad research areas which would usually cause the research to be classified as ‘sensitive’:
   a. Research into illegal activities, research into hate crime, serious crime, fraud, or harmful and illegal cultural practices, the collection of source material from primary sources etc.
   b. Research into illegal or controlled materials e.g. drugs, firearms, bomb making equipment, dangerous chemicals, organisms, GMOs etc that could be used as weapons.
   c. Research which requires access to information which is normally prohibited on University networks, systems and services. This might include (but is not limited to) pornography or the sites of any organisations proscribed by the UK Government; or any research which requires use of the 'dark web' to access information.
   d. Research into extremism and radicalisation.
The above list should not be taken as exhaustive and there may be areas of research not listed that fall within the remit of this Policy.

15. The definition of sensitive research encompasses a wide variety of research topics, and it is a requirement to complete the relevant questions in the Sensitive Research Questionnaire, in order to ascertain if a research project is likely to be considered sensitive research in accordance with this Policy (see Annexes).

16. Research into sensitive, radical or extreme material must be authorised by the University in order to safeguard and protect the researcher, other members of the University community or the University’s corporate reputation. Note: This approval process may not protect individuals from action taken by other countries’ security or legal agencies.

17. Undergraduate and Master’s level research would not normally involve accessing sensitive materials described above but where this level or research is required by the department, the policy will apply.

18. If a proposed student project concerns a sensitive research area, supervisors and Heads of Department should consider whether the student can be appropriately supported in undertaking their research, throughout the course of the research 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 department. This will need to be agreed within the department and IT Services (and Estates if e.g. secure rooms or physical storage is required) before the research takes place.

The Role of the Supervisor(s)

19. Any research project that meets the criteria of sensitive, extreme or radical research must be authorised in accordance with this Policy before research can begin. This will include supporting the researcher in carrying out a Risk Assessment and putting in place mitigating actions to reduce the risk to an acceptable level.

20. For research involving sensitive, extreme or radical research undertaken by any students, supervisors will need to be actively involved in 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 student and colleagues).

Approval Process

21. If the responses to the questionnaire at Annex A identify a research project as ‘sensitive research’, it will require special consideration before approval can be granted. Applicants must demonstrate that they have considered fully the implications of their project and indicated how they will manage and mitigate risks.

22. The lead researcher must complete the questionnaires and, if appropriate, a risk assessment and send the completed forms along with a summary of the project to the Research Ethics and Environment Manager at the email address indicated on the forms. The Research Ethics and

---

Environment Manager will arrange for review of the information by at least two members of the Advisory Group on Sensitive and Extreme Research.

23. The decisions of the Advisory Group will be based on the principles of freedom of speech and academic freedom, in accordance with those policies, and with other relevant policies such as Data Protection and Equality and Diversity.

24. A decision on whether approval will be given will be made by Advisory Group within one month of the submission of the application for approval. The Advisory Group can request additional information or changes to procedures or risk mitigation, and a new one month window begins when the requested additional details are received.

25. Applicants who are refused approval with no option to amend their research design/protocol (something which should be very rare) may approach the Chair of the Advisory Group for further information and advice. If the applicant is still dissatisfied with the outcome, they may appeal in writing to the Pro Vice Chancellor (Research and Enterprise).

26. Any deviation from the research design granted full 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 approval will need to be made. Every effort will be made by the Advisory Group to process this new application as rapidly as possible so as not to delay the research.

27. Details of all forms received will be recorded on a register by the Research Ethics and Environment Manager, along with information on the outcome of requests. The forms, reviewers' comments and other documents will be held on the secure X Drive Filestore for administrative use.

28. The Advisory Group will meet at least once a year to review policy and procedures, suggesting updates and amendments via the University Research Ethics Committee. The Chair of the Advisory Group will be a member of the Research Ethics Committee.

Accessing Sensitive Websites

29. Researchers who access web sites that might be associated with illegal activities, 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. This also applies to sites on what is commonly known as the ‘dark-web’. Accessing these sites may also affect an individual’s application for security clearance in the future.

30. There are a number of Proscribed organisations where particular care must be taken when researching into these organisations, this is because the organisation commits or participates in acts of terrorism; prepares for terrorism; promotes or encourages terrorism or is otherwise concerned in terrorism.

31. Once full approval has been granted, researchers must only use the University IT facilities previously agreed (see Para 17) to carry out their research. This will ensure these activities can be identified as a legitimate part of their research. No other University or non-University IT facilities may be used (e.g. home computers or broadband.) However, as stated the University

---

cannot guarantee protection from investigation by external authorities. (In authorised circumstances, non University IT equipment may be used by researchers based off campus, such as overseas Distance Learners, however the risk mitigation processes identified in the Risk Assessment process must be in place.)

32. Should researchers be found to be using any IT facilities that were not agreed as part of the approval process, the project may be halted and the researcher subject to disciplinary proceedings as outlined in Research Code of Conduct.

Storage, Transmission and Destruction of Electronic Material

33. Any data, files or electronic items used or produced during projects that fall under this Policy must be stored appropriately. This will normally be the Research Filestore Service unless a more appropriate location has been agreed with IT Services. No data should be stored on local computers or external storage devices. Destruction of sensitive data must be in accordance with IT Services guidance and the Waste Management policies; where data is stored centrally that will be managed through IT Services.

34. 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.

35. In the instance of collaborative research projects with researchers at other institutions in the UK or abroad, the sharing of documents may be necessary. Where necessary this requirement must be identified during the approval process and a suitable mechanism agreed with IT Services and with Information Assurance Services (e.g. a data sharing agreement may be required). Under no circumstances should any documents associated with sensitive research be transmitted using conventional, unprotected channels (e.g. internet email).

36. Researchers are strongly advised to avoid physically transporting materials connected to sensitive research projects. If it is unavoidable, the approach to transporting the materials must be discussed and agreed in advance with IT Services and/or the Head of Security.

37. Researchers should avoid using personal social media to disseminate critical arguments or the outputs or outcomes of sensitive research projects for the reasons stated above. In particular, it is strongly advised that researchers do not create hyperlinks to sites used (e.g. sites of any proscribed organisations). Additionally, researchers should adhere to the relevant University policies and guidelines relating to use of University Computers, Internet and Social Media.

38. Should researchers be found to be using inappropriate or unauthorised IT facilities or using personal social media to disseminate outcomes, the project may be halted and the researcher subject to disciplinary proceedings as outlined in Research Code of Conduct.

---

5 http://www2.le.ac.uk/offices/itservices/about/policies/regulations
39. Should access be required to data on University facilities, for example by police or security services, Information Assurance Services will be responsible for considering and granting requests and for ensuring access is chaperoned.

**Further Guidance**


42. The University has a Safeguarding Lead and a Prevent Lead who can provide more information on reporting and managing any concerns that researchers or their supervisors may have in regard to this material, details are available on the web site.

43. 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 252 2012), or email (SecurityOffice@le.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.

**Training**

44. Training in Safeguarding and Preventing Radicalisation is available to all staff through an e-learning package and additional training can be made available through the Safeguarding and Prevent Leads. Training in completing Risk Assessments can be provided by the University’s Safety Services.

**Breach of the Policy**

45. Breach of this Policy through failure to gain approval for sensitive research, deviation from the research design originally submitted for approval, or failure to store or transmit research materials securely, forfeits any protection the University can offer should external authorities launch an investigation. Normally breaches of this policy by staff will be investigated through the Research Code of Conduct and Ordinance 23 – Discipline, while those for students will be investigated via the relevant Senate regulation.

---

6 [http://www2.le.ac.uk/offices/ias](http://www2.le.ac.uk/offices/ias)
7 [http://www2.le.ac.uk/offices/researchsupport/full-code-of-conduct](http://www2.le.ac.uk/offices/researchsupport/full-code-of-conduct)
8 [http://www2.le.ac.uk/offices/sas2/regulations/senate-regulations](http://www2.le.ac.uk/offices/sas2/regulations/senate-regulations)
Update and Review

46. This version approved June 2016. Next review scheduled 2017.