UNIVERSITY OF LEICESTER

Policy on Researching and Handling Sensitive, Extreme or Radical Material

Document Control

Prepared by (lead responsibility)	Paul Cullis, Chair of the University Ethics and Integrity Committee Rob Dover, Associate Professor in Intelligence and Security Shaun Monkman, Ethics and Integrity Manager
Approved by	Research and Enterprise Committee
Date of issue	25/06/2021
Version	2
Next review date	25/06/2023

Policy development steps

Action	Description of steps taken
Legal implications of this policy area	This policy was created by a working group of interested parties and approved by Senate in 2016. This version has had a light touch review to ensure that the policy is in line with the latest legislation and guidance. It has been out for further consultation internally as below.
Consultation for this policy	This policy has been reviewed by and received input from: • Safeguarding Lead • Head of Security • Prevent Lead • Health and Safety Services • Legal Services • Research Ethics, Governance and Integrity Team

Version History

Version 1 – June 2016	First version of the policy
Version 2 – 25 June 2021	Light touch review of version 1, transfer to new template and separation of policy from procedure

Related procedures/guidance:

- AG-SERM-SOP-1 - Procedure for Managing SERM Applications
- Handling or Researching Sensitive, Extreme and Radical Material Application Form
- Research Code of Conduct
- Research Ethics Policy
- Ordinance 23 – Discipline
- Internet Code of Practice
- Information Security Policy Documents

1. Introduction

1.1. 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 this type of 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.

1.2. The University carries out a wide range of activity 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.

1.3. It is a duty of the University to ensure research into radical, sensitive 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. This includes research involving chemicals or organisms that can be used as weapons. See Section 6 for a definition

1.4. All projects that meet the criteria for researching such material as defined in this policy **must** be approved by the Advisory Group on Research and Handling Sensitive, Extreme and Radical Material prior to starting.

1.5. 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.

1.6. 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, the Research Ethics Policy and Research Code of Conduct for further details.

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

2. Scope

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

2.2. 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
- undergraduate and postgraduate students (both taught and research), whether registered here or on temporary placement.

2.3 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.

2.4 It should be noted that researchers based overseas, or researchers travelling to overseas locations, will need to abide by local laws and regulations regarding collecting and holding material covered by this policy. 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.

2.3. **Note:** This approval process may not protect individuals from action taken by other countries' security or legal agencies.

3. Legal Implications

3.1. The collection, recording, possession, viewing on the internet, distribution, etc of security sensitive research material may be interpreted as committing an offence under the provisions of section 58 of the Terrorism Act 2000 and the Terrorism Act 2006 if not confined to use for purely academic research purposes

4. Monitoring and review:

4.1. This Policy will be reviewed every 2 years by the Advisory Group on Research and Handling Sensitive, Extreme and Radical Material

4.2. Compliance will be monitored by the Advisory Group on Research and Handling Sensitive, Extreme and Radical Material

5. Duties and Responsibilities

5.1. 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.

5.2. Supervisors must ensure they understand their role, and ensure they provide suitable support to those who carry out research and may be vulnerable to harming themselves or others through their actions; this is termed 'safeguarding'.

5.3. Researchers or others undertaking activity covered by this policy are responsible for ensuring they understand their role and obtain approval for their project from the Advisory Group on Research and Handling Sensitive, Extreme and Radical Material prior to starting work.

5.4. Senior researchers, including, but not limited to: Principal Investigators, Doctoral and Dissertation Supervisors, and Heads of College/Schools , 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.

5.5. The Advisory Group on Research and Handling Sensitive, Extreme and Radical Material are responsible for reviewing applications, providing support, guidance and approval of projects covered by this policy.

5.6. The Chair and members of the Advisory Group on Research and Handling Sensitive, Extreme and Radical Material will be appointed by the Chair of UEIC with advice from members of UEIC and subject to ratification from the Research and Enterprise Committee.

6. Sensitive, Extreme and Radical Material

6.1. There are four broad research areas which would usually cause the research to be covered by this policy:

- Research into illegal activities, such as:
    - Platforms where membership or engagement could result in a police or security service investigation and sanctions;
    - Interviews, focus groups, surveys, or correspondence with members of proscribed groups, those who self-identify allegiance to proscribed groups, or who have been convicted of offences concerning the object of study
- 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
- Research into illegal or controlled materials e.g. drugs, firearms, bomb making equipment, dangerous chemicals, organisms, including genetically modified ones that could be used as weapons.
- Research into extremism and radicalisation

6.2. The definition of sensitive research encompasses a wide variety of research topics, and it is a requirement to complete the relevant questions in the Research and Handling Sensitive, Extreme and Radical Material Application Form, in order to ascertain if a research project is likely to be considered sensitive research in accordance with this Policy.

6.3. 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. This authorisation may only be provided in the form of approval from the Advisory Group on Sensitive, Extreme or Radical Research.

6.4. Note: This approval process may not protect individuals from action taken by UK or other countries' security or legal agencies.

6.5. Undergraduate and Masters level research should not normally involve accessing sensitive materials described above. In exceptional circumstances, where research of this nature is required by the School this policy will apply.

6.6. If a proposed student project concerns topics covered by this policy, supervisors and Heads of School 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 student's School . This will need to be agreed within the School and IT Services (and Estates if e.g. secure rooms or physical storage is required) before the research takes place.

7. The Role of the Supervisor

7.1. 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. The supervisor is responsible for supporting the researcher in carrying out a Risk Assessment and putting in place mitigating actions to reduce the risk to an acceptable level. They are also responsible for ensuring checks on the mitigations to ensure they are effective throughout the life of the project.

7.2. For research involving sensitive, extreme or radical material 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 the student and colleagues).

8. The Role of the Researcher

8.1. Any researcher or other person whose project may be covered by this policy should complete the Research and Handling Sensitive, Extreme and Radical Material Application Form to ascertain if approval is required.

8.2. If the outcome of the questionnaire is that approval is required by the Advisory Group, then they should send the Application Form for review by the Advisory Group, following the procedures provided on the Research and Handling Extreme, Sensitive an Radical Material web pages for submitting their application to the Advisory Group.

8.3. The researcher should work with the Advisory Group to ensure that all risks relating to their project, that are specific to the material they are working with, are identified, controlled and managed. They should respond to the Group in a timely manner to ensure effective and speedy review of their application.

8.4. Once approval has been gained, the researcher must obtain further approval from the Advisory Group if they wish to deviate from the agreed project plan.

8.5. Researchers must obtain approval from the Advisory Group prior to gaining ethical approval for their project. Confirmation of approval must be provided to the Research Ethics Committee.

9. The Role of the Advisory Group

9.1. 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.

9.2. A decision on whether approval will be given will be made by the 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.

9.3. Applications requiring completion of Part 1 of the application form may be approved using Chair's action.

9.4. Applications requiring completion of Part 2 of the application form will be reviewed by a minimum of two Advisory Group members.

9.5. Where two Advisory Group members are not able to agree on a course of action, the application should be escalated for review by the whole panel.

9.6. 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).

9.7. 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.

9.8. Details of all forms received will be recorded on a register by those administering the Advisory Group, 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.

9.9. The Advisory Group will meet at least once a year to review policy and procedures, suggesting updates and amendments via the University Ethics and Integrity Committee.

9.10. The Advisory Group will operate in line with a Terms of Reference agreed by the University Ethics and Integrity Committee

9.11. The Chair of the Advisory Group will be a member of the University Ethics and Integrity Committee.

10. Accessing Sensitive Websites

10.1. 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.

10.2. 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.

10.3. Once full approval has been granted, researchers must only use the University IT facilities previously agreed 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 Learning students, however the risk mitigation processes identified in the Risk Assessment process must be in place.)

11. Storage, Transmission and Destruction of Electronic Material

11.1. 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. Further guidance is available on Research Records Retention.

11.2. 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.

11.3. 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).

11.4. 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.

11.5. 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.

11.6. 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.

12. Breach of the Policy

12.1. Should researchers be found to be using any IT facilities that were not agreed as part of the approval process, or using social media for dissemination of findings, the project may be halted and the researcher subject to disciplinary proceedings.

12.2. 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 in accordance with Senate Regulation 11.

12.3. 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.

13. Further Guidance

13.1. Guidance on security-sensitive material has been issued by Universities UK in a document entitled 'Oversight of security-sensitive research material in UK universities: guidance', dated October 2012.

13.2. Guidance on dealing with material that could potentially radicalise the researcher or those associated with the researcher is part of the Government's 'Prevent Agenda' and the University is required to comply with the Prevent Duties which are contained in the 'Prevent Duty Guidance for higher education institutions in England and Wales', dated July 2015.

13.3. 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.

13.4. 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.

14. Investigations and Enquiries

14.1. If anyone has concerns related to the use or misuse of sensitive, extreme or radical 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.

14.2. The Ethics and Integrity Manager will support the Head of Security and the Chair of the Advisory Group with both internal university enquiries, and police enquiries, about suspect security sensitive material associated with a university or a university member. Such material will be treated as having a legitimate research purpose unless the material or the relevant researcher and approved project cannot be identified.