Edge Hill University

Policy on researching and handling sensitive material

Contents

Introduction 1
Scope of this policy 2
Duties and responsibilities 3
What is 'sensitive research'? 3
The role of the supervisor(s) 4
Approval process 4
Accessing sensitive websites 5
Storage, transmission and destruction of electronic material 6
Further guidance 7
Training 7
Breach of the policy 8
Update and review 8

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 you must follow appropriate processes for conducting the research and storing the related research materials. This policy is a sub-policy of the University's Code of Practice for the Conduct of Research (Research CoP).
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 you 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 CoP 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 through the ethical approval process.
7. The process for accessing, using and storing data related to research into extreme, radical and/or security-sensitive material should be clearly identified in a data management plan established at the outset of the project.
8. 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 chemicals, but is intended to function alongside these other existing requirements.

Scope of this policy

9. This policy applies to the following:
    a. Full time, part time or agency staff in any role, including honorary appointments and emeritus professors
    b. Staff visiting from other institutions undertaking or supervising research at or for the University
    c. Undergraduate and postgraduate students (both taught and research), whether registered here or on temporary placement.
10. The term ‘researcher’ is used in this policy as a general term to cover all of the above groups.
11. 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.
12. 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 your responsibility to familiarise yourself 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 you from action taken by other countries’ security or legal agencies.**

Duties and responsibilities

13. You have a duty 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.

14. 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’.

15. 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 CoP and this policy before the research is conducted.

What is ‘sensitive research’?

16. 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.

17. 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.

18. 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 (SRQ; available on request from the Research Office), in order to ascertain if a research project is likely to be considered sensitive research in accordance with this policy.

19. 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 you from action taken by other countries' security or legal agencies.

20. Undergraduate and master's level research would not normally involve accessing sensitive materials described above but where this level of research is required or approved by the department, the policy will apply.

21. 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. The department should identify any special provisions, facilities or resources such as IT access to normally prohibited sites or secure storage of materials. If you are engaged in such work, you must complete an IT Services *Application to access sensitive content form*, which must be approved by the Chair of the University Research Ethics Sub-committee (URESC) before any research can commence. This will need to be agreed within the department and IT Services (and Facilities Management if e.g. secure rooms or physical storage is required) before the research takes place.

The role of the supervisor(s)

22. 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.

23. For research involving sensitive, extreme or radical research undertaken by students, you will need to be actively involved in the students' work and support 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

24. If the responses to the SRQ identify a research project as 'sensitive research', it will require special consideration before approval can be granted. You must demonstrate that you have considered fully the implications of your project and indicated how you will manage and mitigate risks. See also the Research Ethics Policy for guidance on the appropriate approval process for research projects.

25. The lead researcher/principal investigator must complete the SRQ and a risk assessment as part of the ethics application which needs to be submitted to URESC to be reviewed by the full committee. When ethics applications including access to sensitive materials are received, the University's Prevent Lead (the Deputy Director of Student Services) will be invited to attend the meeting to review the application.

26. The decisions of URESC 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.

27. Details of all forms received will be recorded on a register by the secretary of URESC, along with information on the outcome of requests. The forms, reviewers' comments and other documents will be held in a secure folder for administrative use.

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

29. If you are refused approval with no option to amend your research design/protocol, you may approach the Chair of URESC for further information and advice. If you are still dissatisfied with the outcome, you may appeal in writing to the Pro Vice Chancellor (Research).

30. Any deviation from the research design that was 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 revised submission for ethical approval, addressing specifically the issue of sensitive materials, will need to be made. Every effort will be made by URESC to process this new application as rapidly as possible so as not to delay the research.

31. URESC will review policy and procedures on sensitive materials annually, suggesting updates and amendments for approval by the University Research Committee. Such proposals will also be reviewed by the University's Prevent Lead.

Accessing sensitive websites

32. If you access web sites that might be associated with illegal activities, radicalisation or terrorist/extremist organisations or groups, you should be conscious that such sites may be subject to surveillance by law enforcement agencies, 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 application you make for security clearance in the future.

33. There are a number of proscribed organisations where particular care must be taken; for example because the organisation commits or participates in acts of terrorism; prepares for terrorism; promotes or encourages terrorism or is otherwise concerned in terrorism.

34. Once full approval has been granted, you must only use the University IT facilities previously agreed to carry out your research. This will ensure these activities can be identified as a legitimate part of your research (see para 19). 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, you may use non-University IT equipment when based off campus; however the risk mitigation processes you identified in the Risk Assessment process must be in place.)

35. Should you be found to be using any IT facilities that were not agreed as part of the approval process, the project may be halted and you will be subject to disciplinary proceedings as outlined in the Research CoP.

Storage, transmission and destruction of electronic material

36. Any data, files or electronic items used or produced during projects that fall under this policy must be stored appropriately. This will normally be a secure, centrally provided folder 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 the University Information Security Policy and identified in your data management plan; data stored centrally will be managed through IT Services.

37. You should note that the Terrorism Act (2006) and the Counter-terrorism and Security Act (2015) outlaw the dissemination of terrorist publications with 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.

38. 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 Governance Services (based in the Strategic Planning and Policy Unit) 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).

39. You 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 Facilities Management.

40. You 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 you do not create hyperlinks to sites used (e.g. sites of any proscribed organisations). Additionally, you should adhere to the relevant University policies and guidelines relating to use of University computers, internet and social media.

41. Should you be found to be using inappropriate or unauthorised IT facilities, or using personal social media to disseminate outcomes, the project may be halted and you will be subject to disciplinary proceedings as outlined in the Research CoP.

42. Should access be required to data on University facilities, for example by police or security services, Information Governance Services will be responsible for considering and granting requests and for ensuring access is chaperoned.

Further guidance

43. 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. This is available at universitiesuk.ac.uk/policy-and- analysis/reports/Documents/2012/oversight-of-security-sensitive-research-material.pdf

44. 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. Available here: gov.uk/government/uploads/system/uploads/attachment_data/file/445916/Prevent_Duty_Guidance_For_Higher_Education__England__Wales_.pdf.

45. The University has a Safeguarding Lead (the Director of Student Services) and a Prevent Lead (the Deputy Director of Student Services) who can provide more information on reporting and managing any concerns that you or your supervisors may have in regard to this material, details are available on the web site.

46. 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 staff member's head of department or the student's supervisor. Where this is not possible, please contact the relevant dean. Should 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 Campus Support Team verifies whether these materials relate to a legitimate research project.

Training

47. 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 Research Risk Assessments can be provided by the University's Research Office.

Breach of the policy

48. 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 Code of Practice for the Investigation into Research Misconduct, while those for students will be investigated via the relevant regulations.

Update and review

This policy was approved by the University Research Committee on 25 October 2017.