Terrorism and Extremism-Related Research Policy (Taught Students)

Contents

Alternative format

If you require this document in an alternative format, please contact the Research, Enterprise and Scholarship Unit.

Email: research-integrity@open.ac.uk

Summary of policy

This policy sets out the duties of the University and students who are conducting research connected to terrorism, extremism and radicalisation while studying at The Open University, involving the collection, recording, possession, viewing on the internet or distribution of Security-Sensitive Research Materials. This applies to students carrying out independent research, such as for a dissertation module.

Scope

Who this policy covers

This document applies to all students studying taught undergraduate modules and qualifications and postgraduate students registered for taught qualifications, or studying modules that form part of a taught qualification.

It is also intended to support Module Teams and Associate Lecturers by providing guidance on how students should be supported in researching these topics.

Who this policy does not cover

This policy does not apply to Open University staff, postgraduate research students, research carried out in collaboration with other organisations and research by visiting and emeritus academics who are conducting externally or internally funded research at or on behalf of The Open University. Such research is instead covered by a separate Terrorism and Extremism-Related Research policy.

The Open University Student Charter Values

The Student Charter was developed jointly by The Open University and the OU Students Association. It is a declaration of our shared values and the commitments we make to each other. This document has been developed with the Student Charter values as its foundation.

Related Documentation

Please refer to the following documentation in conjunction with this document:

- OU Ethical Research Statement

- OU Statement of Principles on Academic Freedom

- OU Prevent Principles

- OU Student Computing Policy

- OU Academic Conduct Policy

- OU Code of Practice for Student Discipline

Relevant legislation:

- The Terrorism Act (2006)

- The Counter-Terrorism and Border Security Act (2019)

- UK Government's Definition of Extremism (2024)

Introduction

As a Higher Education Institution (HEI), The Open University (OU) conducts a wide range of research. The OU Principles on Academic Freedom state that:

'All members of the University's academic community, both students and staff, have freedom within the law to hold and express opinions, question and test established ideas or received wisdom, develop and advance new ideas or innovative proposals, present controversial or unpopular points of view'.

However, where research is being conducted on issues relating to security-sensitive, radical or extreme topics, particular care is needed. The Terrorism Act (2006) and the Counter-Terrorism and Security Act (2019) outlaw the dissemination of terrorist publications and the viewing or otherwise accessing via the internet documents or records containing information likely to be useful to a person committing or preparing an act of terrorism, regardless of intent.

It is the duty of students, and the University, to ensure that research conducted by taught students in these areas is legitimate, carried out appropriately, and takes account of the requirement, including that set out in law, to safeguard both the student and wider society. This policy sets out the duties of the University and the student in this area.

You should read through this policy carefully. For specific advice on how this document applies to your own work, please seek advice from your tutor or supervisor. Tutors or supervisors should refer any queries to the Module Team in the first instance, and if the Module Team require further support, they should consult with the Associate Dean Research and/or the Research Governance Team.

Email: research-integrity@open.ac.uk

Policy

1. Purpose

It is an offence in UK law to view or otherwise access via the internet documents or records containing information likely to be useful to a person committing or preparing an act of terrorism. There is an allowable defence if the information/material being viewed or downloaded is being used for approved, academic research purposes.

The objectives of this policy are to clearly set out the duties and responsibilities of the University and students who are conducting or planning to conduct research connected to terrorism[1], extremism[2] and radicalisation while studying at The Open University, where this requires accessing and/or storing Security-Sensitive Research Materials.

2. The Open University's Responsibility

2.1 The University has a responsibility to protect its staff and students working on legitimate and approved academic research in areas of terrorism and extremism that requires access to terrorism, extremism or other Security-Sensitive Research Materials, including but not limited to those of proscribed organisations. The University has a responsibility to protect its staff and students from both the possible radicalising effects of viewing such materials, and from the misinterpretation of intent by law enforcement agencies (which may result in prosecution and/or other sanctions against the researcher).

2.2 The Module Team Chair(s) and the student's Associate Lecturer have a responsibility to ensure the student's wellbeing and safety, while also enabling legitimate research into terrorism and extremism-related topics. The Module Team Chair(s) should ensure that

---

1 For the purposes of this policy, 'Terrorism' corresponds to the UK government definition of terrorism in the Terrorism Act 2006 (summarised in the 'Glossary' section of this document).
2 For the purposes of this policy, 'Extremism' corresponds to the UK government definition of extremism set out in March 2024 (summarised in the 'Glossary' section of this document).

students have access to this guidance, and that the Module supports students to develop appropriate research into terrorism and extremism-related topics, with appropriate risk mitigation.

2.3   In order to fulfil these responsibilities, the University needs to be aware of and review all research being carried out that falls into the category of terrorism and/or extremism-related research. Where the research will involve accessing and/or storing security sensitive materials, institutional approval (via the University's Ethical Research Review Body – see glossary) must be obtained before any extremism-related research commences. The University will maintain a central register of all such research.

3.   The Responsibility of Students

3.1   Students have a responsibility to ensure that before commencing any research in the area of terrorism or extremism that might involve accessing and/or storing security sensitive materials,[3] the project proposal is subject to review and institutional registration (see [Section 4](#)).

3.2   Where students intend to research terrorism and extremism-related topics solely through module materials, the secondary academic literature and online material which cannot reasonably be considered 'security-sensitive', such as openly accessible government policy documents, then this would not require review and registration.

3.3   However, if there is *any* possibility that a student could access Security-Sensitive Research Material as a part of their research, such as looking at the social media communications of proscribed organisations, or viewing the websites and propaganda of extremist groups, then they must submit their research proposal for review and registration to their Module team. Where the review identifies that the research will involve accessing and/or storing security sensitive materials, the student is responsible for ensuring that institutional approval is obtained before commencing the project. This is to ensure their maximum protection when viewing or accessing (including download and storage) terrorism or extremism-related research materials for legitimate and approved academic research purposes.

---

3 Please see the 'Glossary' for a definition of 'security sensitive research material'.

3.4 While this document sets out how the University can manage the risks associated with students researching terrorism and extremism-related topics, not all research that falls within this area of study can be supported for taught students.

3.5 Students will necessarily be working to shorter research timescales than members of staff, and research students and will not have access to the training and support required for higher risk research in this area.

3.6 As such, in the context of taught provision, the University will not be able to support research that involves:

3.6.1 Contact with members of proscribed groups, or individuals convicted of terrorism offences, whether this be in person or through electronic communication (e.g., email, social media).

3.6.2 Accessing and/or storing explicit, violent or grotesque imagery.

3.6.3 Research that would require security sensitive material to be transferred or accessed by anyone other than the student.

3.7 Institutional approval must be obtained before commencing the research (see Section 4).

3.8 Students have a responsibility for ensuring security sensitive research material is accessed and managed according to the principles set out in this policy.

3.9 Students should be aware of the personal risks of exposing themselves to extremist or terrorism related materials, for example propaganda, recruitment and/or violent materials (as outlined in the OU's counter terrorism ('Prevent') training), and carefully consider risk mitigation strategies (see 3.10 below).

3.10 Risk mitigation strategies should be set out in the Module 'Ethics' process and in the Terrorism and Extremism-Related Research (Taught Students) Registration and Approval Form (see Section 4). Students should seek advice from their Associate Lecturer and Module Team Chair if they have concerns or queries as to how to best manage the risks associated with terrorism and extremism-related research.

3.11 All students conducting research into terrorism or extremism-related topics are required to undertake the OU's counter terrorism ('Prevent') training before commencing any research.

4. Project Registration and Approval

4.1 In order for the University to carry out its duties as required under the counter-terrorism legislation and Prevent duty, and to ensure its students are protected from misinterpretation of intent and/or wrongful prosecution, any research projects connected with terrorism, extremism and/or radicalisation are required to undergo a project review before the research can commence. Where the review identifies that the research involves accessing and/or storing security sensitive materials, the project is required to undergo an approval process.

4.2 Research which involves accessing and/or storing security sensitive materials will be subject to review by the Open University Ethical Research Review Body (ERRB). The research cannot commence until it has been approved by the ERRB. Any changes to the project will require re-approval by the ERRB.

4.3 This guidance recognises that each module will have its own ethics review process. It is expected that the approval process for terrorism or extremism-related research takes place in addition to existing module practices. As part of the terrorism or extremism-related research approval process, ERRB will require evidence the student has engaged fully with the Module 'Ethics' process (which will usually mean a completed 'Ethics Review' form), and that this has conditionally been approved by the Module Team.

4.4 Students are required to submit the Terrorism and Extremism-Related Research (Taught Students) Registration and Approval Form alongside the Module 'Ethics' process to their Module Team for review. When, and if, the Module Team conditionally approve the overall project, the Module Team will submit the Terrorism and Extremism-Related Research (Taught Students) Registration and Approval Form, alongside the Module 'Ethics Review' form (or equivalent), as well as Counter-terrorism (Prevent) training records of completion for the student, the Module Team chair, and the supervising AL, as well as any other supporting documents, to research-integrity@open.ac.uk for review by the ERRB.

4.5 If ERRB requires adjustments to the research for approval to be granted, the student would revise their 'Research Ethics' form and/or their Terrorism and Extremism-Related Research (Taught Students) Registration and Approval Form. These would then be resubmitted back to the Module Team, who would review changes, before sending them on to the ERRB via the research-integrity@open.ac.uk mailbox for further scrutiny. This process would repeat until all necessary adjustments are made and approval is granted.

5.   Accessing and storing security sensitive online content

5.1   Students should be aware that extremist and terrorist-related websites may be under surveillance by law enforcement agencies. Accessing/viewing and/or downloading Security-Sensitive Research Materials, particularly if they are terrorism or extremism-related, may be illegal and viewed as a prosecutable offence if it is not for approved, academic research purposes (regardless of any actual illegal intent).

5.2   Section 58 of the Terrorism Act 2000 made it an offence if a person 'collects or makes a record of information of a kind likely to be useful to a person committing or preparing an act of terrorism'. Sections 2 and 3 of the Terrorism Act 2006 outlaws the dissemination of terrorist publications, including by electronic means. A modification of the Counter-Terrorism and Border Security Act 2019 also introduced the offence of viewing or otherwise accessing via the internet documents or records containing information likely to be useful to a person committing or preparing an act of terrorism. There is, however, a defence if the information is used for approved academic research purposes.

5.3   Registration, review and approval of the research by the University (see the process described in [Section 4](#)) allows the University to confirm and provide evidence, if required, that the activity is part of legitimate and approved academic research work. Institutional approval must be obtained before commencing the research.

5.4   Particular care must be taken to appropriately access and store Security-Sensitive Research Materials. Students must establish a data management plan – communicated in Section 4 of the Terrorism and Extremism-Related Research (Taught Students) Registration and Approval Form – that accords with the principles set out below.

5.5   All research materials, including data, files or other digital or electronic items including audio or video material used or produced in the course of terrorism and extremism-related research must be stored securely, in a password protected file. It should not be possible for anyone else to access this material.

5.6   You must not transmit or exchange (e.g., send via email or any other messaging system) any security sensitive material.

5.7   You should connect to the internet via a private network, and not a public Wi-Fi.

5.8   Physical materials such as manuals, reports or other hard copy documents should be scanned and uploaded to the password protected file, and the original hard copy destroyed.

5.9   Once your research project has been completed, you must destroy all collected data and materials. Students should contact [Information Security](#) for advice on secure data destruction.

---

6.   Transmitting Security-Sensitive Research Materials

6.1   Sections 2 and 3 of the Terrorism Act 2006 outlaws the dissemination of terrorist publications, including by electronic means.

6.2   In the context of taught student provision, there is generally no reasonable need for sensitive material to be transferred or accessed by anyone except the student.

6.3 As such, sensitive research material and data should not be transmitted or exchanged, and no one else should be allowed access to the sensitive material. In exceptional circumstances, where the student's Associate Lecturer (tutor) or Module Team Chair requires access to the sensitive research materials, for either academic or safeguarding purposes, the student should contact research-integrity@open.ac.uk for advice and assistance with this.

---

7.   Student Safety

7.1   Any research concerning terrorism and extremism carries risks. There is a risk that security services may become aware of the student accessing Security- Sensitive Research Material and may not realise that the access is related to their legitimate and approved academic research. The student then may become a target for surveillance and possible further security service action.

7.2   The registration process is designed to mitigate this risk. If security services or law enforcement raise concerns with the student or University, the University would be able to confirm that the student was accessing material as an approved part of their research.

7.3   There is also a risk to the wellbeing of the student. Research in this area carries the potential to access or see graphic and/or violent text or images, whether intentionally or unintentionally. These can cause psychological harm to the student. Finally, there is an inherent safeguarding risk. Through engaging with violent or extreme material, the student concerned could be at risk of radicalisation.

7.4   To manage the latter two risks it will be necessary for a tutor or module team member to conduct additional wellbeing checks with students researching these topics through the course of the independent research. Depending on the length of the independent

research, it is expected that this might amount to 2-3 check-ins over the course of a module.

7.5   These check-ins should solely be to assess the wellbeing of the student. The member of staff should inquire into how the research is going with the student, and ask whether they have any concerns or challenges that they wish to raise or discuss.

7.6   If a wellbeing concern is raised by the student or the member of staff, this is an opportunity to either flag up support available through the OU, or to directly refer the student to relevant support services.

7.7   If a safeguarding risk is identified by the student or member of staff, and there are concerns around radicalisation, the member of staff should refer this to the OU Prevent Co-ordinator.

7.8   If the student fails to arrange or attend these check-ins, the tutor or module team member should use their judgement, but may wish to consider sharing any concerns with relevant student support services or the OU Prevent Coordinator.

---

8.   Further Information

8.1   **Registration Process for Terrorism and Extremism-related research**

To register your project, complete the Terrorism and Extremism-related Research (Taught Students) Registration and Approval Form and submit it to your Module Team, in line with their Module Ethics process.

8.2   **Approval Process for Terrorism and Extremism-related research involving access to and/or storage of security sensitive materials**

Where it is identified the project will involve access to and/or storage of security sensitive materials, the submitted documentation will be considered by the Ethical Research Review Body (ERRB) (link). The research must not commence until it has been approved by the ERRB. Any changes to the project will require re-approval by the ERRB, following reconsideration by the Module Team, in line with their Module Ethics process.

8.3   **The Prevent duty**

Further information on the University's approach to the Prevent duty can be found on the Prevent (Counter-terrorism) Duty pages

Questions or comments regarding any aspects of the University's response to the Prevent duty, can be addressed to the OU Prevent Co-ordinator.

8.4   Raising concerns

Concerns relating to the use or misuse of sensitive research material by any student or member of University staff should be raised by contacting the OU Prevent Co-ordinator.

8.5   Breach of the policy

Breaches of the Policy by students will be dealt with through the relevant student conduct and/or disciplinary -related policies and procedures.

Commitment to Equality, Diversity and Inclusion at The Open University

Policies are inclusive of all Open University staff and Open University students, regardless of age, care experience, caring status or dependency, civil status, disability, family status, gender, gender expression, gender identity, gender reassignment, marital status, marriage and civil partnership, membership of the Traveller community, political opinion, pregnancy and maternity, race, religion or belief, sex, sexual orientation, socio-economic background or trades union membership status.

Safe Space Reporting

The Open University is committed to creating a diverse and inclusive environment in which everyone feels safe and is treated with dignity and respect. Unlawful discrimination of any kind across The Open University will not be tolerated. Safe Space Reporting is available through an online tool through which staff, students, learners and visitors are encouraged to report incidents of assault, bullying, harassment, hate crime, or sexual harassment. It also provides information about what you can do if these incidents happen to you, or to someone you know, and where you can find support.

Glossary

Terrorism
The current UK definition of terrorism is given in the Terrorism Act 2006. In summary this defines terrorism as the use or threat of action that endangers or causes serious violence to a person/people; causes serious damage to property; or seriously interferes or disrupts an electronic system. The use or threat must be designed to influence the government or to intimidate the public and is made for the purpose of advancing a political, religious or ideological cause.

Extremism

The [UK Government definition of Extremism (2024)](#) defines Extremism as: 'the promotion or advancement of an ideology based on violence, hatred or intolerance, that aims to:

1. negate or destroy the fundamental rights and freedoms of others; or
2. undermine, overturn or replace the UK's system of liberal parliamentary democracy and democratic rights; or
3. intentionally create a permissive environment for others to achieve the results in (1) or (2).

Proscribed organisations

Organisations which may be prosecuted under UK law. The [UK government website](#) contains a list of currently proscribed organisations. Note that organisations not yet included on this list that have recently started to promote terrorist or extremist agendas may also be prosecuted under this legislation.

Radicalisation

The process by which a person comes to support terrorism and forms of extremism leading to terrorism.

Security Sensitive Research Material

Although there is no legal definition of 'security sensitive', research material which could be classified as "security-sensitive" may include anything which could be interpreted as promoting, endorsing or planning terrorism, radicalisation, or extremism. It is therefore not possible to provide an exhaustive list or description of what might be considered 'security-sensitive' and an element of judgment will be required. However, 'security-sensitive' information is likely to include (but not necessarily be limited to) material relating to:

- Extremism e.g. material that results from collecting information from websites of extremist organisations.
- Terrorism e.g. material gained through gathering content on actual or potential terrorist methods.
- Radicalisation e.g. material obtained by liaising with groups which seek to persuade young people to adopt extreme political, religious, or social views.
- Government security measures in respect of extremism, terrorism or radicalisation (other than government sponsored research) e.g. an analysis of government techniques to combat terrorism, where such information would be of use to terrorists.

Further clarification

For specific guidance on how this document applies to your own research, please seek advice from your tutor or supervisor. Tutors or supervisors should refer any queries to the Module Team in the first instance, and if the Module Team require further support, they should consult with the Associate Dean Research and/or the Research Governance Team.

Email: research-integrity@open.ac.uk

If you have any comments about this policy document and how it might be improved, please submit these to research-integrity@open.ac.uk.

Document Information

Version number: 1.0

Approved by: Student Experience Committee

Effective from: 1 November 2024

Date for review: November 2025