Terrorism and Extremism-Related Research Policy

Contents

Summary of policy

This policy sets out the duties of the University and individual researchers conducting research connected to terrorism, extremism and radicalisation on behalf of the Open University, involving the collection, recording, possession, viewing on the internet, distribution, etc. of security- sensitive research materials[1]. This includes external and internally-funded research, research by staff and postgraduate research students, research carried out in collaboration with other organisations and research by visiting academics.

Summary of significant changes since last version

The policy has been updated to make it clear that 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 may be illegal if it is not for **approved** academic research purposes (regardless of intent) and that institutional **approval** must be obtained before commencing research involving accessing such materials. Previously, researchers were only required to register their research in this area.

The policy has been updated to clarify that all security sensitive extremism and terrorism related research material should normally be stored on a secure, centrally managed SharePoint site.

Scope

Who this policy covers

This document applies to all 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.

Staff conducting research, staff managing those who conduct research, postgraduate research students and their supervisors are therefore required to understand and comply with this policy.

Who this policy does not cover

This document does not apply to students studying taught undergraduate modules and qualifications or postgraduate students registered for taught qualifications, or studying modules that form part of a taught qualification. Taught students with queries on how their studies may be impacted by the matters outlined in this policy should contact the OU Prevent Co-ordinator.

[1] See glossary for definitions and further information on what may constitute ‘security-sensitive’ materials.

Equality, Diversity and Inclusion

Policies are inclusive of all Open University staff and Open University postgraduate research 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.

Related Documentation

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

- OU Research Code of Practice
- OU Procedure for dealing with allegations of academic malpractice or misconduct
- OU Plagiarism and Research Misconduct Policy (Postgraduate Research Students)
- OU Research Data Management Policy
- OU Ethical Research Statement
- OU Statement of Principles on Academic Freedom
- OU Prevent Principles
- OU Information Security Policies

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*'.

The OU Code of Practice for Research sets out the standards that govern the conduct of research at the OU and includes a requirement for researchers to comply with all legal and ethical requirements relating to their research.

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 individual researchers, and the University, to ensure that research in these areas is legitimate, carried out appropriately, and takes account of the requirement, including that set out in law, to safeguard both the researcher and wider society. This policy sets out the duties of the University and the individual researcher in this area.

You should read through this policy carefully. For specific advice on how this document applies to your own research, please seek advice from your Associate Dean Research, supervisor 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 individual researchers who are conducting or planning to conduct research connected to terrorism[2], extremism[3] and radicalisation on behalf of the Open University, where this requires accessing and/or storing security-sensitive research materials. This includes external and internally-funded research, research carried out in collaboration with other organisations and research by visiting academics.

2. The University's Responsibility

The University has a responsibility to protect researchers 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 those of proscribed organisations. The University has a responsibility to protect its researchers 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).

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. The University will maintain a central register of all such research. Where the research will involve accessing and/or storing security sensitive materials, institutional approval must be obtained before any extremism-related research commences.

[2] 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).
[3] For the purposes of this policy, 'Extremism' corresponds to the UK government definition of extremism in the PREVENT Strategy (2011) (summarised in the 'Glossary' section of this document).

The University will also provide a secure, centrally managed SharePoint site where security sensitive research material can be stored, and a clear policy on the management of such material

---

3. The Responsibility of Researchers

Researchers have a responsiblity to ensure that **before** commencing any research in the area of terrorism or extremism, the project proposal is subject to review and institutional registration. Where the review identifies that the research will involve accessing and/or storing security sensitive materials, the researcher is responsible for ensuring that institutional approval is obtained **before** commencing the project. This is to ensure their maximum protection when viewing, accessing (including download and storage) terrorism or extremism-related research materials for legitimate and approved academic research purposes.

Institutional approval must be obtained before commencing the research.

Researchers have a responsibility for ensuring security sensitive research material is kept off personal computers and is instead stored in the secure, centrally managed Open University SharePoint site set up for this purpose. It must be accessed and managed according to the principles set out in this policy.

Researchers should be aware of the personal risks of exposing themselves to extremist or terrorism related materials, for example propaganda, recruitment and/or violent materials, and carefully consider risk mitigation strategies.

All OU staff and postgraduate research students are required to undertake the OU's counter terrorism ('Prevent') training every two years. You must ensure you are up to date with this training before commencing any research in the areas of terrorism or extremism.

---

4. Project Registration and Approval

In order for the University to carry out its duties as required under the counter-terrorism legislation and Prevent Duty, and to ensure its researchers 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 and institutional registration process 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.

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.

If your research project involves human participants or human data, including online interaction with, or observation of humans, or observations of the traces they leave through social media or other platforms, e.g. Twitter, Facebook etc, then your project additionally requires review by the Human Research Ethics Committee (HREC). HREC review should take place prior to ERRB project registration and approval.

5. Accessing security sensitive online content

Researchers should be aware that extremist and terrorist-related websites may be under surveillance by law enforcement agencies. Accessing/viewing such (proscribed) websites and /or downloading security-sensitive 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 internet). Registration, review and approval of the research by the University (see the process described in paragraph 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.

Once approval has been obtained, researchers must use the Open University network to access such material online to ensure that these activities are recognised by law enforcement agencies and other authorities as integral to the approved research project.

6. Storing Security-Sensitive Research Materials

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 outlaw 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.

Particular care must therefore be taken to appropriately store security-sensitive research materials and data. Researchers must establish a data management plan that accords with the principles set out below.

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 in the secure, centrally managed Open University SharePoint site set up for this purpose. Only those with a legitimate reason to access the materials will be given the necessary permissions to the site. Materials (including copies) should not normally be kept in any other location. The materials should not be transmitted or exchanged.

Where it is not possible to store materials on the SharePoint site, for example when working off-line, it is allowable to ***temporarily*** store the materials on a University-managed personal computer, University-managed laptop or University encrypted portable storage device. Using an OU-managed computer/laptop, preferably fully-optimised, means that it is encrypted so the data that is stored on it is protected should the device be lost or stolen.

If researchers need to work on their research data and materials away from the OU network using their OU computer/laptop, they should use OU IT-approved remote access protocols to connect to the University's network. Public Wi-Fi connections should not be used.

Physical materials such as manuals, reports or other hard copy documents should be scanned and uploaded to the SharePoint secure area, and the original hard copy destroyed.

Once your research project has been completed, you must follow OU policy in relation to the archiving and retention or destruction of data and materials. Researchers should contact Information Security for advice on secure data destruction.

For further information, advice and guidance, please contact Information Security via information-security@open.ac.uk.

---

7. Transmitting Security-Sensitive Research Materials

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

Sensitive research material and data should not be transmitted or exchanged, rather it should be stored on a centrally managed SharePoint site. Those with legitimate reason to access the materials (internal or external research collaborators) will be given the necessary permissions to the site.

Where a researcher intends to work with external research collaborators, arrangements for data storage, data management and data access should be clearly set out in the collaboration agreement.

The collaboration agreement must be concluded, and institutional approval obtained before the research may commence.

---

8. Further Information

Registration Process for Terrorism and Extremism-related research

To register your project, complete the Extremism and Terrorism-related Research Project Registration Form (link) and submit it with any supporting documentation to: research-integrity@open.ac.uk.

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 may 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 Human Research Ethics Committee, where applicable.

The Prevent Duty

Further information on the University's approach to the Prevent Duty can be found on the Prevent intranet 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.

Raising concerns

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

Breach of the policy

The requirements set out in this Policy form part of the OU Research Code of Practice, and breaches of the Policy by University staff and visiting academics will be dealt with via the Procedure for dealing with allegations of academic malpractice or misconduct. Breaches of the Policy by postgraduate research students with be dealt with via the Plagiarism and Research Misconduct Policy (Postgraduate Research Students).

Glossary of terms

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 Prevent Strategy (2011) defines extremism as vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. We also include in our definition of extremism calls for the death of members of our armed forces, whether in this country or overseas.

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 refers to 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 Associate Dean Research, supervisor and/or the Research Governance Team within the Research, Enterprise and Scholarship Unit.

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.

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

Version number: 2.1	Approved by: Research Committee
Effective from: 1 June 2022	Date for review: March 2024
Contact: research-integrity@open.ac.uk	