RESEARCH INVOLVING TERRORIST OR VIOLENT EXTREMIST MATERIAL

1.0 PURPOSE

The Counter-Terrorism and Security Act 2015 places a duty on Universities to have "due regard to the need to prevent people from being drawn into terrorism". This requires the University to have appropriate policies and procedures in place for projects which will utilise violent extremist materials, and to identify and address issues where such materials are accessed for non-legitimate purposes. This document sets out requirements relating to the use of such materials for research, in line with advice provided by Universities UK.

The University supports both its academic faculty and the student body in undertaking research utilising materials that may be considered 'security-sensitive' in this context, but takes seriously its responsibility to protect them from the potentially radicalising effects of viewing materials of this type and of misinterpretation of intent by authorities (which may result in legal sanction).

To ensure the University is able to protect its researchers it must be aware of and approve the research before it begins. Early notification is through the ethical review process; it is from this that the institution is able to ensure proper data governance and oversight.

2.0 SCOPE

In the context of this document the term 'security-sensitive' is used to designate:

- Materials which are covered by the Terrorism Acts of 2000 and 2006 and the Counter-Terrorism and Security Act 2015.

Such materials include those produced by groups currently proscribed by the UK government as terrorist organisations, or by other groups which advocate the use of violence to achieve their aims.

Where researchers are unclear whether the sources utilised in their research fall within the scope of this legislation, they should in the first instance seek advice from their supervisor (in the case of students), or departmental ethics officer (in the case of staff), who may refer to the Deputy Lead Safeguarding Officer for advice where required.

3.0 ETHICAL REVIEW

The University is clear that research involving the access, collection and use of security-sensitive materials carries a risk to researchers as well as the general public and therefore any such research must be subject to ethical review.

All University staff and student research ethics questionnaires, must:

a) Identify relevant projects which
   i) Involve the study of an organisation which is proscribed under the terms of the Terrorism Act, or require accessing materials produced by or in support of such an organisation (see https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations--2)
   ii) Involve the study of any other current organisation which, as part of its agreed programme, advocates the use of violence to achieve its aims, or require accessing materials produced by or in support of such an organisation.

b) Provide a supplementary form (Appendix A) to be completed for those projects so identified, to be submitted alongside the completed questionnaire.

Following ethical approval, Heads of Department must sign off such projects and Research & Innovation Services (R&IS) should be notified.

4.0 DATA GOVERNANCE

When accessing security sensitive material, researchers should be aware that there are circumstances where use (and further dissemination) of this material may be illegal (i.e. in breach of legislation), or unlawful (i.e. in breach of a website's terms and conditions of use). Concerns that proposed use of material may contravene legal or contractual obligations should be referred to Legal Services for advice.

Researchers should be aware that websites containing security-sensitive materials may be under surveillance by the authorities and that accessing them and / or downloading related materials may lead to police enquiries.

Security sensitive research material should not be kept on personal computers, personal cloud storage, or in non-secure locations.

When a requirement to store security-sensitive material is identified, a request should be made to the University's Computing & Information Services to set up a suitable storage location for the researcher(s) involved in the project. By using a designated secure file store (along with appropriate ethics approval), the researcher will ensure that, if required, the University can confirm that the materials within it are being used for legitimate purposes.

Security-sensitive material in hard copy should be stored in a secure location, or scanned and uploaded to the secure file store and the paper copy securely destroyed.

Materials within the file store must not be circulated to anyone outside the research project or transmitted by insecure means.

Secure file stores are intended primarily for source materials, and it is not expected that researchers store their own writing about security-sensitive material within this location unless that, too, is considered best kept out of circulation.

University IT facilities should be used when accessing any security-sensitive websites, thereby helping to ensure that access is flagged as being a legitimate part of research and ensuring that enquiries come to the institution in the first instance. Additional guidance on accessing online materials is available.

5.0 OVERSIGHT

The University has a responsibility to consider the welfare of all staff and students, and to offer advice and support to researchers who may be adversely affected (emotionally or intellectually) by the research that they undertake. Individuals also have a responsibility to consider the potential impacts of their research (on themselves, or on those with whom they may share it), and should seek advice and support as needed. Any concerns should be raised as soon as possible.

In the case of student projects, in the first instance it is the project supervisor's responsibility to consider the welfare of the students. Supervisors should share concerns with their line manager, or a responsible person in the relevant department or college in the first instance.

In the case of staff projects, the Head of Department should share concerns with Human Resources in the first instance.

The University provides training on safeguarding from radicalisation, which can be accessed via Durham University Online (duo).

6.0 CONTACTS

Any queries from legitimate bodies e.g. the police or security services should be directed to the University's Deputy Lead Safeguarding Officer in the first instance, and Research & Innovation Services should be informed.

Where a member of staff requires further advice or support with a proposal related to security-sensitive research, they should contact their departmental ethics representative, who may escalate queries to Research & Innovation Services to direct as appropriate.

RELATED DOCUMENTS

- Safeguarding policy
- IT Regulations
- Research Conduct and Integrity Policy

DOCUMENT ADMINISTRATION

Current Status	
Version:	1.0
Approval date:	29 November 2016
Approved by:	Senate
Owner:	Research & Innovation Services
Review date:	November 2018

APPENDIX A: SUPPLEMENTARY FORM

The Terrorism Act (2006) outlaws the dissemination of records, statements and other documents that can be interpreted as promoting or endorsing terrorist acts. To fulfil its obligations under the Counter-Terrorism and Security Act 2015, the University requires safeguards around research involving materials originating from organisations considered by the UK government to be terrorist (referred to as 'proscribed organisations'), or from other current organisations which advocate the use of violence to achieve their aims.

1. Please list the relevant organisations from which you will access material (or materials which support them), highlighting any organisations on the UK government's list of proscribed organisations: https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations--2

2. Does your research involve the storage of any such records, statements or other documents?

Yes ☐ No ☐

3. Might your research involve the electronic transmission of such records or statements?

Yes ☐ No ☐

4. If you answered 'Yes' to questions 2 or 3, you are advised to store the relevant records or statements electronically on a secure university file store. The same applies to paper documents with the same sort of content. These should be scanned and uploaded. Access will be restricted to individual(s) involved in the research project with a legitimate need to access the material. Please indicate below that you agree to store all documents relevant to questions 2 and 3 on that file store:

Yes ☐ No ☐ If you answered no, please give your reason:

4a. Please indicate below that you agree not to transmit (electronically or by any other means) documents in the file store to anyone outside the research project:

Yes ☐ No ☐ If you answered no, please give your reason:

5. Will your research involve visits to websites that might be associated with violent extremist, or terrorist, organisations?

Yes ☐ No ☐

6. If you answer 'Yes' to question 5, you are advised that such sites may be subject to surveillance by the police. Accessing those sites might lead to police enquiries. Please acknowledge that you understand that this is a potential consequence by putting an 'X' in the 'Yes' box.

Yes ☐

6a. Please indicate below that you have read and understood the University's guidance on accessing sites relating to terrorism or violent extremism.

Yes ☐

6b. Please indicate below that you agree to use University IT facilities when accessing such sites.

Yes ☐ No ☐ If you answered no, please give your reason:

7. In the event of enquiries by the security services, Research & Innovation Services may require access to a list of titles of documents (but not the contents of documents) in the document store and a record of sites visited. Please acknowledge this by putting an 'X' in the 'Yes' box.

Yes ☐

APPENDIX B: GUIDANCE ON ACCESSING SITES RELATING TO TERRORISM OR VIOLENT EXTREMISM

Carrying out research into topics relating to terrorism or violent extremism should normally be unproblematic, for example research that uses books, journal articles, think-tanks, media and other easily recognised accessible sources. Research may become problematic only if you need to access sites which contain materials considered by the UK government to endorse or promote terrorism or violent extremism. Such sites may

- encourage terrorism by directly or indirectly inciting or encouraging others to commit acts of terrorism. This includes an offence of "glorification" of terror – praising or celebrating terrorism in a way that may encourage others to commit a terrorist act.
- provide assistance in preparing or carrying out acts of terrorism, for example by promoting the sale, loan, distribution or transmission of terrorist publications, e.g. a bomb-making manual.
- advocate the use of violence.

You can still access these sites if it is necessary for your work, but you should be aware of the potential problems and take the necessary actions to avoid them.

Staff and students planning to access such websites are advised that such sites are likely to be subject to surveillance by the police and intelligence services, and that accessing them might lead to police enquiries.

The UK Terrorism Acts of 2000 and 2006 and the Counter-Terrorism and Security Act 2015 introduced offences relating to the collection, possession, transmission or distribution of 'information of a kind likely to be useful to a person committing or preparing an act of terrorism'. Under the Counter-Terrorism and Security Act 2015, safeguards are also required around materials which it is considered may aid radicalisation. It is permissible to collect/possess such information if one has 'a reasonable excuse for his action or possession'. Academic research falls under this category and is permissible.

There are two categories of material you may be dealing with:

a) those which are, or may be, illegal to possess without a reasonable excuse
b) those which are legal, but which may have repercussions if used or distributed in an inappropriate way, and which may in some cases bring you to the attention of the authorities.

When working with material which expresses extreme, and potentially violent, views, researchers have a responsibility to consider the potential distress or other harm which such material could cause if shared without due consideration or if accidentally viewed by others. The University requires particular safeguards around any materials produced by groups characterised by violent extremism. While not necessarily proscribed by the government in all cases, such groups are likely to advocate or endorse activities that are illegal.

To reiterate, academic research which engages with material in either category is permissible. However, if you have concerns that proposed use of the material within your research project may be illegal, you should contact Legal Services for advice. In addition, you should always also check any terms and conditions associated with the website you are using to ensure that the proposed use for research purposes is not prohibited by the terms of use. Again, in the event that you are concerned that proposed use of material may be unlawful (i.e. in breach of a website's terms and conditions of use), please contact Legal Services for advice.

To protect yourself, you should:

1. Ensure you have notified the University of your intention to carry out research involving materials produced by groups considered by the UK government to be terrorist or which

advocate violent extremism. This is normally done via the ethical review forms issued by your department.

If, as your research develops, you find that you need to access terrorist or violent extremist materials which you had not originally anticipated, and which are not covered by any ethical approval you have received, you should seek advice from your departmental ethics officer and where necessary submit a new ethics application.

2. Check any terms and conditions associated with the website you are using, and seek advice if you are concerned that the work you propose to carry out may conflict with the terms of use.
3. Use University IT facilities to access the websites – do not use your home internet connection. This includes any web searches which you think are likely to lead you to such sites. To avoid causing concern or distress to others, make sure that you view the material in an area which gives protection from accidental viewing by others.
4. Only download the minimum amount of information necessary to fulfil your research assignment, ensuring that all such information can be clearly shown to be relevant to the declared research assignment.
5. Only store any downloaded materials in the secure file store provided by the University. NB Researchers are not required to store their own writing about security-sensitive material within the store, but may do so if they wish to ensure that it is kept out of circulation.
6. Not print or distribute by any means any information downloaded from such websites.
7. Don't communicate with anyone associated with such websites (including via social media), unless this has been explicitly approved as part of the ethical review process.
8. Print out a record of websites visited with dates and the reason for visiting the site, including any documents downloaded. (This will only need to be produced should your activity raise concern with the intelligence services or the police).
9. Destroy any downloaded material once it is no longer required.
10. If, in the course of your research, you become aware of an individual's or group's intention to commit offences relating to terrorism, you have a legal duty to report this immediately.

For some research topics, you may not anticipate dealing with terrorist or violent extremist material, but you may carry out online searches which could lead unintentionally to sites containing such materials. This should not stop you carrying out your research, but you should think about the search terms you are using and consider whether your search results may contain such sites. You are advised to use University IT facilities to carry out such searches (see point 3 above). If you accidentally access material that you believe may be security-sensitive, you should note the circumstances of the visit and raise any concerns with your supervisor (or departmental ethics officer).