OVERSIGHT OF SECURITY-SENSITIVE RESEARCH MATERIAL IN UK UNIVERSITIES

GUIDANCE

Universities UK

CONTENTS

EXECUTIVE SUMMARY

Universities play a vital role in carrying out research on issues where security-sensitive material is relevant. This guidance document concerns the storage and circulation of security-sensitive research material. If circulated carelessly, such material is sometimes open to misinterpretation by the authorities, and can put researchers in danger of arrest and prosecution under, for example, counter-terrorism legislation.[1] Procedures for independently registering and storing this material – through research ethics processes – are recommended in this guidance.

RECOMMENDATIONS

- Procedures for dealing with security-sensitive research in UK universities **should be embedded in research ethics approval processes**. This might involve questionnaires for researchers at universities (templates for which are provided in Annexe A and Annexe B).

- 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. Such security sensitive research material **should therefore be kept off personal computers and stored instead on specially designated university servers** supervised by university ethics officers (or their counterparts) at one remove from university authorities. This material could be accessed easily and securely by researchers, and would not be transmitted or exchanged.

- **Ethics officers (or their counterparts) should be a first, or early, point of contact for both internal university enquiries and police enquiries about suspect security-sensitive material** associated with a university or a university member. Such material should be treated as having a legitimate research purpose unless ethics officers (or their counterparts) cannot identify it or the relevant researcher responsible for it.

- The mechanism for storing security-sensitive material described above needs to be operated alongside **comprehensive advice from universities to all university-based internet users,** highlighting the legal risks of accessing and downloading from sites that might be subject to provisions of counter-terrorism legislation. Reading this advice should be a condition of getting a university email account.

- **A training scheme should be offered to ethics officers (or their counterparts) and IT officers** in universities about implementing the ethics review process and secure storage of sensitive material. Prevent leads should be involved in this training where relevant.

1 See section 58 of the Terrorism Act 2000 as amended by sections 3 and 7 of the Counter-Terrorism and Border Security Act 2019, and sections 2 and 3 of the Terrorism Act 2006. Section 2 of the Terrorism Act 2006 has been amended by sections 5(6) and 5(7) of the Counter-Terrorism and Border Security Act 2019.

1. BACKGROUND

This publication is an updated version of guidance that was first published in 2012, following (i) ongoing discussions among stakeholders in security research in the UK; and (ii) the Universities UK report *Freedom of speech on campus: rights and responsibilities in UK universities* (UUK, 2011). That report highlighted the crucial role that universities play in undertaking research in areas related to security, terrorism and resilience. It also acknowledged that carrying out such research requires particular care to be taken to avoid any infringement of the law.

Professor Tom Sorell of the University of Birmingham was first commissioned to write this guidance in consultation with the higher education sector. Universities UK has subsequently made minor revisions to the guidance to reflect legislative changes, drawing on legal advice.

2. SCOPE OF THE GUIDANCE

This guidance:

- outlines specific ethical issues arising in this area and provides a template for a questionnaire that universities might incorporate into an ethics approval process
- offers a model for a typical internal university rapid response process if problems do occur, which might be used by institutions to adapt practices and processes
- outlines what training might involve for university ethics officers (or their counterparts) in adapting or applying the model.

3. SECURITY-SENSITIVE MATERIAL: THE ISSUES

As part of the government's Prevent strategy (HM Government, 2011), which seeks to 'stop people becoming terrorists or supporting terrorism', the government is committed to supporting universities and other institutions and sectors in their counter-terrorism activities. The government's *Prevent duty guidance: For higher education institutions in England and Wales* (HM Government, 2019) invokes section 26(1) of the Counter-Terrorism and Security Act 2015, which imposes a duty on 'specified authorities', when exercising their functions, to have due regard to the need to prevent people from being drawn into terrorism. Universities must be vigilant in relation to ensuring that they are carrying out their Prevent-related duties, including following rigorous policies and procedures, but care must also be taken to ensure that researchers and students handling security-sensitive material for legitimate reasons are appropriately protected.

There is a range of legislative provisions that relate to the storage and circulation of security-sensitive material. Section 58 of the Terrorism Act 2000 makes 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'. A modification by 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 which is likely to be useful to a person committing or preparing an act of terrorism. There is a defense if the information is used for academic research purposes. Steps therefore need to be taken to ensure that individuals handling security-sensitive research for legitimate purposes do so exclusively for those purposes so as not to come under the suspicion of the police.

Sections 2 and 3 of the Terrorism Act 2006 also outlaw the dissemination of terrorist publications, including by electronic means, and give a very wide definition of 'terrorist publication' and 'statements' that could be construed as encouraging or inducing the commission preparation or instigation of acts of terrorism. Academic research is not a defense under the Terrorism Act 2006.

Sector discussions have identified a number of general issues related to security-sensitive material. An al-Qaeda manual, for example, can be highly relevant to many kinds of perfectly legitimate academic research – studies of jihadism, international relations, or conflict and security, to name three. On the other hand, prosecutions under counter-terrorism legislation in the UK have sometimes been brought on the basis of an accumulation on personal computers of downloaded material and other data, for example that which is relevant to making explosives. It will not always be possible for police to distinguish immediately between the accumulation of such material for legitimate research purposes and the accumulation of material for terrorist purposes.

Researchers may not only download material that is security-sensitive, but also visit security-sensitive websites. Such visits may be interpreted by police as evidence of sympathy for, and perhaps even willingness to collude with, terrorism.

University researchers trying to carry out security-sensitive projects in a legal environment that is highly attuned to the demands of counter-terrorism need protection from intrusive and excessive oversight where this is possible. Consultation with stakeholders suggests that this could best be achieved by research oversight processes within universities. Such processes could expedite checks within universities which would reveal people as legitimate researchers and sensitive material as part of legitimate projects. The same processes could also speed up the identification of material that was outside the area of official research, and that might require further investigation.

Not all security-sensitive research relates to terrorism, and some universities will have little or no such research being conducted. Security-sensitive research could be associated with work on military equipment that has been commissioned by the Ministry of Defence, with extremism from animal rights campaigners, or with IT encryption design for public bodies or businesses, to give only a few examples. Universities will have to decide locally and transparently what 'security-sensitive research' covers.

Researchers apart, many students in universities may visit extremist sites out of curiosity, and may exchange material downloaded or copied from these sites for a variety of reasons, including their own amusement. Communication of this material can be interpreted as contravening counter-terrorism legislation in the UK. Although the objective of this guidance is to indicate means of protecting legitimate research from official intrusion and misinterpretation, it is natural to connect this task with the broader one of protecting harmless internet use in universities that innocently strays into security-sensitive areas. This is discussed in section 5.

4. DEALING WITH THE ISSUES IN RESEARCH

Research staff and students in UK universities have for many years been required to subject their work to ethical review. Initially, this review process mainly applied to medical research. Ethical review aimed to prevent avoidable harm to animal subjects, and violations of autonomy in ill-informed or otherwise vulnerable human subjects. Later, ethical review spread to other research areas. The ethical review questionnaire process could be expanded to include declaration of research in security-sensitive areas, including terrorism (see Annexe A). The general ethical justification for doing this is straightforward: unauthorised acquisition and use of security-sensitive information can carry risks to the public, and even legitimate researchers can be suspected of obtaining it and using it in ways that can be harmful, with costs to those researchers. Oversight helps to prevent both kinds of harm.

To declare as a student or member of academic staff that one is using security-sensitive information is in keeping with openness in research, and helps to reduce misidentifications of information-gathering as suspect or criminal. Besides requiring the declaration itself, universities might provide secure storage of security-sensitive material on a university server overseen by their ethics officers[2] or suitable counterparts in universities without ethics officers (e.g. heads of research ethics committees or data protection officers). Central and secure storage – and a convention among researchers of not exchanging files from this store with others – would keep security-sensitive material off personal computers, and would shield the material from unjustified external scrutiny and misinterpretation. This would be no more onerous than what is presently required in some universities.

A mechanism for registering declarations of security-sensitive research is not a mechanism for reviewing this research, or regulating it; it is a mechanism that operates on already approved research and merely identifies it as a candidate for safe storage.

The Terrorism Act 2006 provides a wide definition of 'terrorist publication' and 'statements' and outlaws their dissemination, including by electronic means. Reference to the definitions of 'terrorist publication' and 'statements' might need to be included as guidance for declarations of use of security-sensitive material for research purposes only (see Annexe B). Registration of the use of this material might be no more difficult than ticking boxes on an online form on a university research ethics website. Registration would result in a researcher being issued with a link to a password-protected documents file on a central university server to which one could upload security-sensitive research documents. These documents could be accessed only by the researcher, and would be subject to a norm of non-circulation.

Ethics officers or their counterparts overseeing the store would not know more than the document titles on the server and the names of researchers. In this way, research would be kept secure and at arm's length from police, in return for openness on the part of researchers about their use of security-sensitive material, all of which they would keep in the store.

4.1 ITEMS IN THE SAFE STORE

A store of security-sensitive material on a university server will mainly contain documents that, as with certain versions of al-Qaeda manuals, can be downloaded from the internet or are otherwise publicly available. These are not secret documents, but rather documents that, if found on personal computers or as attachments in covertly observed email traffic, may throw suspicion on computer owners or senders of email. The purpose of the store on the server is to identify the material as being for research and to keep it out of any further circulation. The store may contain not only documents that were originally in electronic form – some may be scanned versions of paper documents that, again, might look suspicious to an outsider if found on someone's desk. The store would not typically

2 Normally, the academic chairs of research ethics committees, as opposed to administrative staff connected to research ethics committees

function as a repository for an individual researcher's writing about security-sensitive material, unless that, too, was considered best kept out of circulation and was therefore deposited by the researcher.

4.2 SECURITY ENQUIRIES TO ETHICS OFFICERS AND RAPID RESPONSE PROCESS

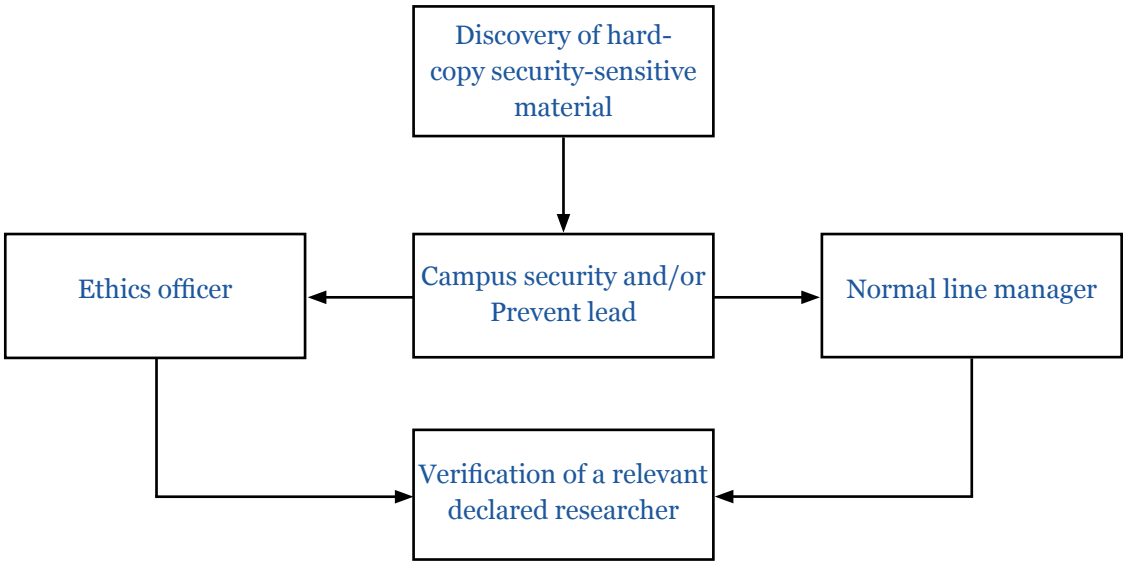
Ethics officers or their counterparts would know who was carrying out declared security-sensitive research in a university, and so would be in a position to confirm whether or not an individual found to possess such material was a declared researcher with a good reason for using it. On the other hand, ethics officers would not know what the research content was in any detail, and would not communicate even the titles of stored documents, unless required to do so by law officers.

Supervisors of research student users of the store would know what the research content was as a result of the normal postgraduate research supervision process; so would heads of department in the case of researchers on the staff of universities. However, supervisors and heads of department would be at one remove from ethics officers or their counterparts. In many cases, confirmation by ethics officers of declared researcher status would be enough to reassure anyone interested that the storage of material was legitimate and not to be interfered with. Or, if an ethics officer himself or herself needed more reassurance, he or she could approach the relevant supervisor or head of department. In any case, declared researchers would have at least two layers of protection from non-university intrusion: ethics officers and heads of department. Depending on the policy of the individual university, ethics officers or their counterparts would be first or early points of contact for both internal and external enquiries about discovered research-sensitive material.

INTERNAL ENQUIRIES

Internal enquiries would probably start with the unexpected discovery by someone of security-sensitive material in an inappropriate place. Although the scope for the unexpected discovery of such material in an inappropriate electronic location would be limited under the mechanism proposed, hard-copy material might still raise questions and might be in circulation even under the proposed mechanism, although it is discouraged in the proposed draft online advice (see Annexe B, question 3). University advice (see Annexe D) might be – this is one possible model only – that discovered material of this kind should first be taken to campus security and/or the Prevent lead, themselves previously briefed about the policy on security-sensitive material, who could then contact his or her normal line manager and the ethics officer for verification of a relevant declared researcher (Figure 1).

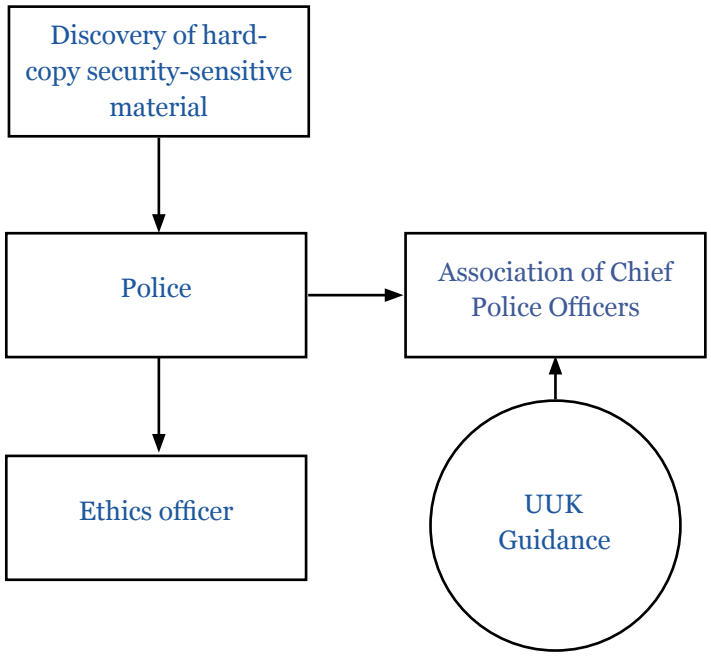
FIGURE 1: INTERNAL ENQUIRIES



EXTERNAL ENQUIRIES

Enquiries from the police that arise from their own discovery or an externally reported discovery of security-sensitive material associated with a university or university researcher could also start with the ethics officer of the university concerned (Figure 2), in liaison with the university's Prevent lead. It would aid this approach if universities were to share their procedures in this regard with the local police and provide a first point of contact – this should form part of routine engagement with the police on campus safety and crime prevention (Association of Chief Police Officers (ACPO), 2012). Properly briefed in this way, the police are likely to treat suspect university-associated material as innocent until proven otherwise.

FIGURE 2: EXTERNAL ENQUIRIES



University ethics officers themselves might offer both voicemail and email contact for external and internal queries. The voicemail would offer a checking service: a service to determine whether or not material found somewhere was associated with a declared researcher and research project.[3]

4.3 THE APPROPRIATENESS OF USING THE ETHICS REVIEW PROCEDURE

Not only is ethics approval a well-known and easy-to-adapt part of the process of monitoring university research in the UK, but ethics officers are credible contact points for the authorities and credible custodians of university research stores. Ethics officers – probably senior academics who head research ethics committees – or their counterparts could be designated first-contact points in all universities for enquiries about security-sensitive material discovered on university computers. Ethics officers have networks that extend across the UK,[4] and work in many or most universities. This makes it straightforward to offer them training on a national basis in security-sensitive research issues, and to roll out a system of oversight of such research in most UK universities.

3 Enquirers could be directed to an online form (see Annexe E) via which they could submit their concerns, creating a written record. Draft responses would be copied to a registrar and/or pro-vice-chancellor's office and/or head of department before being authorised for release to the enquirer. Fuller police enquiries would be referred to these university authorities from the start.

4 The relevant body here is the Universities Ethics Sub-Committee of the Association of Research Ethics Committees (AREC). AREC has a second sub-committee dealing primarily with NHS research.

Even when it is a condition of getting ethics approval for research that applicants agree to use a secure, central research store for security-sensitive documents, there will always be researchers who ignore or break the rules and, perhaps for principled reasons, refuse to be open about the material they are using. These people opt out of the mechanism and do so at a cost: if the use of central security stores becomes widespread, the discovery of undeclared, security-sensitive research material will cast more suspicion on a researcher than it would (as now) if there were no mechanism for handling it. So, for the self-protection of researchers, it is wise to use the secure central store.

5. A SECOND, COMPLEMENTARY MECHANISM

It is not only researchers who need protection from scrutiny and arrest when they use security-sensitive material legitimately, but also non-researchers in universities, including undergraduates. They may access this material for academic purposes, but they may also turn to it out of personal curiosity and download it with no malicious intent. Such individuals would not normally be subjected to a research ethics process or checks by an ethics officer to clear the material of suspicion.

The right response to the danger of official misinterpretation of this material is not to create more central stores for non-researchers. Rather, pointed guidelines are needed for all internet users at universities and more exacting conditions for acquiring email accounts at, and internet access from, universities. University guidance for all internet users can call attention to the risks of visiting and downloading from jihadist websites. Behaviour that seems to ignore this advice might be punished with the loss of email privileges.

Guidance issued in the future by all UK universities might promise the same consequences for frivolous visits to, and downloading from, jihadist sites, as well as for frivolous exchanges of material obtained from these sites.

Such guidance is not fool proof, but it should be no easier to ignore than existing rules for internet use in a given university. Once again, the message sent out from universities to students and staff would be that, for one's own protection, one should not invite the attentions of the police by visiting such sites. Advice to all university-based internet users about the dangers of accessing and storing security-sensitive material, and about the sheer breadth of the legal definitions of material that might have the effect of encouraging terrorism (see Annexe B), concerns all or most people in universities, and not just researchers.

By providing clear advice and research-specific mechanisms, universities will minimise the risk of difficulties arising from individuals accessing sensitive material for legitimate purposes.

6. STIGMATISATION

It can be anticipated that some security-sensitive material will be associated with Islamic studies researchers, and perhaps other social science researchers who identify themselves as Muslim or other faiths.

Do the proposed mechanisms single out specific groups? No. The research ethics process will involve all postgraduate and some staff research relevant to the Terrorism Act (see the initial questions proposed for online security-sensitive research review at Annexe A). It will also extend to a broad range of security-sensitive material – such as military research and research promoting counter-terrorism. The existence of a research ethics review process and the availability of safe storage for security-sensitive material will not stigmatise any specific groups.

7. ETHICS OFFICERS AND INFORMATION TECHNOLOGY (IT) COLLEAGUES

Since the mechanism suggested in section 4 of this guidance involves a secure server, it will carry some administrative and monetary costs to universities. On the administrative side, it requires ethics officers to be able to get from IT colleagues clear descriptions for researchers of how stored material will be kept secure against intrusion. At the same time, storage should involve the confidential communication to ethics officers of the number and titles of documents stored. This could be done if a directory of titles of documents, as opposed to the documents themselves, could be accessed by ethics officers at any time.

8. TRAINING

Universities implementing the mechanisms described in this guidance may consider providing associated training for both ethics and IT officers, and Prevent leads. A training programme should include:

- a review of current terrorism legislation relevant to research
- suggested contents for forms (electronic and paper) for an ethics approval process
- suggested internet user advice
- what secure server contents would look like when accessed by an ethics officer
- what secure server contents would look like when accessed by a researcher
- what ethics officers should do in the case of a query about security-sensitive research material from
- within their university
- what ethics officers should do in the case of a query from outside their university
- information for IT officers about the hardware and software necessary for a secure, central storage system. The training should also engage the university Prevent lead.

ANNEXE A: TEMPLATE FOR GENERAL QUESTIONNAIRE ON SECURITY-SENSITIVE MATERIAL

Does your research fit into any of the following security-sensitive categories? If so, indicate which by circling the relevant option:

a. commissioned by the military:

Yes No

b. commissioned under an EU security call:

Yes No

c. involves the acquisition of security clearances:

Yes No

d. concerns terrorist or extremist groups:

Yes No

If your answer to question d. is yes, continue to the questions in Annexe B.

ANNEXE B: TEMPLATE FOR ONLINE RESEARCH ETHICS APPROVAL FORM FOR UNIVERSITY RESEARCHERS

The Terrorism Act 2006 outlaws the dissemination of records, statements and other documents that can be interpreted as encouraging or inducing the commission, preparation or instigation of acts of terrorism.

1. Does your research involve the storage on a computer of any such records, statements or other documents?

Yes No

2. Might your research involve the electronic transmission (eg, as an email attachment) of such records or statements?

Yes No

3. If you answered 'Yes' to question 1 or 2, 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 to this file store will be protected by a password unique to you. You agree to store all documents relevant to questions 1 and 2 on that file store:

Yes

3a. You agree not to transmit electronically to any third party documents in the file store:

Yes

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

Yes No

5. If you answered 'Yes' to question 4, you are advised that such sites may be subject to surveillance by the police. Accessing those sites from university IP addresses might lead to police enquiries. Please acknowledge that you understand this risk by circling 'Yes'.

Yes

6. By submitting to the ethics process, you accept that the university ethics office will have access to a list of titles of documents (but not the contents of documents) in your file store. These titles will only be available to the ethics office. Please acknowledge that you accept this by circling 'Yes'.

Yes

Countersigned by supervisor/manager

ANNEXE C: ADVICE ON INTERNET USE FROM A UNIVERSITY IP ADDRESS

The Terrorism Act 2006 outlaws web posting of material that encourages or endorses acts of terrorism. Sections of the Terrorism Act also create a risk of prosecution for those who transmit material of this nature, including transmitting this material electronically.

The storage of such material on a computer can, if discovered, prompt a police investigation.

Again, visits to websites related to jihadism or terrorist websites and downloading of material issued by jihadist or terrorist groups (even from open-access sites) may be subject to monitoring by the police. Storage of this material for research purposes must be registered through the normal research ethics process of the university.

ANNEXE D: ADVICE FOR INDIVIDUALS IN UNIVERSITIES WHO DISCOVER SECURITY-SENSITIVE MATERIAL

FOR A GENERAL AUDIENCE

Some university research involves the use of security-sensitive material, including material related to terrorism and extremism.

Procedures exist for storing this material and not circulating it if it is being used for legitimate research purposes. If you come across material that seems to fit this description, bring it to the attention of the university security office.

FOR UNIVERSITY SECURITY OFFICES

Some university research involves the use of security-sensitive material, including material related to terrorism and extremism.

Procedures exist for storing this material and not circulating it if it is being used for legitimate research purposes.

If such material is handed in, please inform _____* and the research ethics officer.

*Insert name

ANNEXE E: ONLINE FORM FOR ETHICS OFFICE SECURITY ENQUIRIES

This form is to be used to report the discovery within the university of unsupervised material that appears to be security sensitive – in particular, material that might be connected with terrorism and extremism. Material of this kind is sometimes connected with legitimate research projects, and this office carries out checks relevant to establishing whether or not items reported on have that status.

Your name
Your email address
Your contact telephone number
Your enquiry or report

Thank you. This office will contact you and undertake an investigation if necessary.

REFERENCES

ACPO (2012) Prevent, Police and Universities available at: www.safecampuscommunities.ac.uk/uploads/files/2013/05/201205tampreventpandunigui.pdf

HM Government (2011) Prevent Strategy available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf

HM Government (2019) Prevent duty guidance: for higher education institutions in England and Wales available at: www.gov.uk/government/publications/prevent-duty-guidance/prevent-duty-guidance-for-higher-education-institutions-in-england-and-wales

UUK (2011) Freedom of speech on campus: rights and responsibilities in UK universities

Universities UK is the collective voice of 136 universities in England, Scotland, Wales and Northern Ireland.

Our mission is to create the conditions for UK universities to be the best in the world; maximising their positive impact locally, nationally and globally.

Universities UK acts on behalf of universities, represented by their heads of institution.

Universities UK

Woburn House
20 Tavistock Square
London, WC1H 9HQ

+44 (0)20 7419 4111

info@universitiesuk.ac.uk

universitiesuk.ac.uk

@UniversitiesUK

November 2019
ISBN: 978-1-84036-440-8